GFI Product Manual

GFI Network Server Monitor™ Manual

http://www.gfi.com

info@gfi.com

The information and content in this document is provided for informational purposes only and is provided "as is" with no warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. GFI Software is not liable for any damages, including any consequential damages, of any kind that may result from the use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, GFI makes no claim, promise or guarantee about the completeness, accuracy, recency or adequacy of information and is not responsible for misprints, out-of-date information, or errors. GFI makes no warranty, express or implied, and assumes no legal liability or responsibility for the accuracy or completeness of any information contained in this document.
If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.
All product and company names herein may be trademarks of their respective owners.
GFI Network Server Monitor is copyright of GFI SOFTWARE Ltd. - 1999-2011 GFI Software Ltd. All rights reserved.

Document Version: NSM-ACM-EN-01.00.00
Last updated: September 6, 2011

Contents

1 Introduction 1

1.1 Introduction to GFI Network Server Monitor (GFI NSM) 1
1.2 Key features..... 1
1.3 GFI Network Server Monitor components 5
1.4 License scheme 6

2 Installing GFI Network Server Monitor 7

2.1 System requirements 7
2.2 Installation procedure 7
2.3 Entering your license key after installation 13
2.4 Changing NSM Engine Service logon credentials after installation 13

3 Configuring GFI Network Server Monitor 14

3.1 Getting started with GFI Network Server Monitor 14
3.2 Quick Start Wizard 14
3.3 Creating monitor checks 17
3.4 Configure monitor check properties 21
3.5 Inheriting check properties 34
3.6 Enable or disable checks 36
3.7 Testing checks for correctness 36
3.8 Move checks between existing folders 37
3.9 Copy checks from/to existing folders 37

4 Configuring monitor functions 39

4.1 Introduction 39
4.2 Network/Internet monitor functions 39
4.3 SNMP monitoring checks..... 55
4.4 Windows OS generic checks..... 56
4.5 Windows operating system checks 61
4.6 Windows applications checks 73
4.7 Windows OS databases checks..... 76
4.8 Terminal Services checks..... 78
4.9 Linux / Unix OS generic checks 80
4.10 Linux/Unix Operating System Checks 82

5 Check folders 93

5.1 Introduction 93
5.2 Creating new folders..... 94
5.3 Configure properties of existing folders 95
5.4 Deleting folders..... 95
5.5 Moving folders 95
5.6 Searching for folders..... 95

6 Monitoring checks status 97

6.1 Introduction 97
6.2 Viewing the state of checks from the GFI N.S.M. configuration 97
6.3 Viewing the state of checks from the GFI N.S.M. Activity Monitor..... 100
6.4 Viewing the state of checks from a web browser..... 101

6.5 Check state indicators 103

7 Global alerting options 104

7.1 Introduction 104
7.2 Mail server settings 104
7.3 Global settings for network alerts 108
7.4 Global settings for SMS/pager alerts 109
7.5 In-built GSM SMS Server 110
7.6 GFI FAXmaker SMS service provider template 112
7.7 Clickatell Email2SMS Service 113
7.8 Generic SMS service provider template 116
7.9 NSM 5.x/6.0 SMS Server system 118
7.10 Message templates 124

8 General options 127

8.1 Introduction 127
8.2 Uncertain Results settings 127
8.3 Web Server settings 128
8.4 Proxy Server settings 134
8.5 Log file settings 134

9 Database maintenance options 137

9.1 Introduction 137
9.2 Configuring the database backend 137

10 Users and Groups 141

10.1 Introduction 141
10.2 Users 141
10.3 Groups 145

11 Reporting 147

11.1 Introduction 147
11.2 Availability - Detail Report 147
11.3 Availability-Summary Report 150

12 Network tools 153

12.1 Enumerate computers 153
12.2 Enumerate processes 154
12.3 DNS lookup 156
12.4 Whois 157
12.5 Traceroute 158
12.6 SNMP audit 158
12.7 SNMP walk 159

13 Other features 161

13.1 Export configurations 161
13.2 Import configurations 161
13.3 Version information 162
13.4 Licensing 163

14 Writing your own monitoring functions 165

14.1 Introduction 165
14.2 Writing a script/function 165
14.3 Adding a monitor function written in VBscript 166
14.4 WMI (Windows Management Instrumentation) 167
14.5 ADSI (Active Directory Service Interfaces) 167

15 Troubleshooting **169**

15.1 Introduction 169
15.2 Knowledge Base 169
15.3 Web Forum 169
15.4 Request technical support 169
15.5 Build notifications 169

Index **171**

List of screenshots

Screenshot 1 - The GFI Network Server Monitor configuration 6
Screenshot 2 - Previous Version Detected 8
Screenshot 3 - Check for latest build 8
Screenshot 4 – Import settings from an older installation 9
Screenshot 5 - User and License key details 10
Screenshot 6- Service Account details 11
Screenshot 7 - Mail Server details 11
Screenshot 8 - Select a database backend 12
Screenshot 9 – Launching the Quick Start Wizard from the Tools Explorer window 14
Screenshot 10 – Specify the OS of the target computer 15
Screenshot 11 – Specify the services provided by the target computer 15
Screenshot 12 – Specify additional applications that require monitoring 16
Screenshot 13 - Select target computers 16
Screenshot 14 - Select Type of Monitoring Check required 17
Screenshot 15 - ICMP/Ping check properties dialog 18
Screenshot 16 – The Select Computer(s) dialog 19
Screenshot 17 - Logon Credentials dialog 20
Screenshot 18 – The Select Target folder dialog 21
Screenshot 19 - Check properties dialog 22
Screenshot 20 - File existence check parameters 23
Screenshot 21 - Logon Credentials Setup Dialog 24
Screenshot 22 - Actions Setup dialog 25
Screenshot 23- Alerts Setup Dialog 26
Screenshot 24 - Actions dialog with Inherit options enabled 27
Screenshot 25 - Alerts setup dialog 28
Screenshot 26 – Configuring alert recipients 28
Screenshot 27 - Run External File setup dialog 29
Screenshot 28 - File parameters dialog 30
Screenshot 29 - Services / Computer restart setup dialog 31
Screenshot 30 - Dependencies Setup Dialog 32
Screenshot 31 – List of available checks 33
Screenshot 32 - Maintenance schedule Dialog 34
Screenshot 33 - Monitoring check properties - Actions tab setup 35
Screenshot 34 – Check Status display and relative options 36
Screenshot 35 - The 'Monitor Now' dialog 36
Screenshot 36 - HTTP/HTTPS check parameters dialog 39
Screenshot 37 - FTP check parameters dialog 40
Screenshot 38- IMAP server check parameters dialog 41
Screenshot 39 - NNTP Server check parameters dialog 43
Screenshot 40 - POP3 server check parameters dialog 43
Screenshot 41 - SMTP server check parameters dialog 45
Screenshot 42- NTP Time server check parameters dialog 46
Screenshot 43 - DNS server check parameters dialog 47
Screenshot 44 - ICMP/Ping check parameters dialog 48
Screenshot 45 - TCP/IP check parameters dialog 49
Screenshot 46 - Email Route check dialog 50
Screenshot 47 - The test email details dialog 52
Screenshot 48 - SMTP Server configuration dialog 53
Screenshot 49- POP3/IMAP Server configuration dialog 54
Screenshot 50 - SNMP check parameters dialog 56
Screenshot 51 - VBscript check parameters dialog 57
Screenshot 52 - Parameters dialog 57
Screenshot 53 - OS Object Performance Counter check parameters dialog 58
Screenshot 54 - Performance Counter - Object Selection Dialog 59
Screenshot 55 - Command Line Output check parameters dialog 60
Screenshot 56 - Process Properties check parameters dialog 61
Screenshot 57 - Event log check parameters dialog 62
Screenshot 58 - File existence check parameters dialog 63
Screenshot 59 - Disk space check parameters dialog 64
Screenshot 60 - Services check parameters dialog 65
Screenshot 61 – DNS Server Service and display name 65

Screenshot 62 - CPU usage check parameters dialog 66
Screenshot 63 - Directory Size check parameters dialog 67
Screenshot 64 - File size check parameters dialog 68
Screenshot 65 - LDAP Query check parameters dialog 69
Screenshot 66 - Physical Disk check parameters dialog 70
Screenshot 67 - Printer availability check parameters dialog 71
Screenshot 68 – Running Process check parameters dialog 72
Screenshot 69 – Users and Groups check parameters dialog 73
Screenshot 70 - ISA Server check parameters dialog 74
Screenshot 71 - Exchange server check parameters dialog 75
Screenshot 72 - MS SQL/ADO check parameters dialog 76
Screenshot 73 - ODBC administrator with sample database configured 77
Screenshot 74 - ODBC setup with sample database 77
Screenshot 75 - Generic ODBC properties 78
Screenshot 76 – Terminal Services: Port Check parameters dialog 79
Screenshot 77 – Terminal Services: Physical Logon check parameters dialog 80
Screenshot 78 - SSH check parameters dialog 81
Screenshot 79 - The parameters dialog 81
Screenshot 80 - File Existence check parameters dialog 82
Screenshot 81 - CPU usage setup window 83
Screenshot 82 – Directory/folder Size setup window 84
Screenshot 83 - File size check parameters dialog 85
Screenshot 84 - Printer check parameters dialog 86
Screenshot 85 –Running Process check parameters dialog 87
Screenshot 86 – Users and Groups check parameters dialog 88
Screenshot 87 - Disk Partition check parameters dialog 89
Screenshot 88 - Disk Space check parameters dialog. 90
Screenshot 89 - Daemon check properties dialog 91
Screenshot 90 - Nested Folders 93
Screenshot 91 - Folder properties dialog: General Tab 94
Screenshot 92 - Find folder dialog 95
Screenshot 93 – Monitoring Checks status home page 97
Screenshot 94 – The Folder contents page 98
Screenshot 95 - All checks page 99
Screenshot 96 - Nested Folders 99
Screenshot 97 - Engine Status tab 100
Screenshot 98 - Monitoring Check Status tab 100
Screenshot 99 - Remote Monitor: All checks page 101
Screenshot 100 – Monitoring checks status view for mobile devices 102
Screenshot 101 - 'Alerting Options' node 104
Screenshot 102 – Email Alerts configuration dialog 105
Screenshot 103 - Mail server propertiesdialog 106
Screenshot 104 - Format Email Message 107
Screenshot 105 - Network Alerts Properties 108
Screenshot 106 - SMS Alerts dialog 109
Screenshot 107 – The in-built GSM SMS Server properties 110
Screenshot 108 - Edit Property dialog 111
Screenshot 109 - FAXmaker SMS service configuration dialog 112
Screenshot 110 - Clickatell Email2SMS Service configuration dialog 114
Screenshot 111 - Generic SMS service configuration dialog 116
Screenshot 112 – NSM 5 SMS Server configuration dialog 119
Screenshot 113 - Providers tab 120
Screenshot 114 - Dial & Modem properties tab 121
Screenshot 115 - SMSC Provider Setup Screen 122
Screenshot 116 - SMSC providers list 123
Screenshot 117 - SMS/Pager Message Format Window 124
Screenshot 118 – 'General Options' node 127
Screenshot 119 - Uncertain Results setup 128
Screenshot 120 - built in Web Server settings 129
Screenshot 121 - Specifying an alias for the virtual directory 130
Screenshot 122- Pointing to the GFI NSM web folder 130
Screenshot 123 - Setting permissions 131
Screenshot 124 - Setting Virtual Directory properties 131
Screenshot 125 - Specify default document 132

Screenshot 126 - Select authentication method 133
Screenshot 127 - Setting permissions 133
Screenshot 128 - Proxy Server Setup Window 134
Screenshot 129 - Log file setup Window 135
Screenshot 130 - Database Options 137
Screenshot 131 – Ms Access backend properties dialog 138
Screenshot 132 - MSDE/MS SQL Server backend properties dialog 139
Screenshot 133- Users and Groups folders 141
Screenshot 134 - User Properties dialog 142
Screenshot 135 - Working Hours Setup dialog 143
Screenshot 136- Alerts Setup Dialog 144
Screenshot 137- Members of tab 145
Screenshot 138 - Group Properties dialog 146
Screenshot 139 - Specify report interval 147
Screenshot 140 - Select the period to be covered by report 148
Screenshot 141 - Specify which checks to include in the report 148
Screenshot 142 – Choose the report format required 149
Screenshot 143 - The availability detailed report 150
Screenshot 144 - First Stage of the report wizard: Report Type dialog 151
Screenshot 145 - The availability summary report 152
Screenshot 146 - Enumerate computers - General Tab options 153
Screenshot 147 - Enumerate Computers - Advanced tab options 154
Screenshot 148 - Enumerate Processes setup window - General Tab 155
Screenshot 149 – List of Highlighted Processes 156
Screenshot 150- DNS Lookup - setup Window 156
Screenshot 151 - WhoIs tool results 157
Screenshot 152 - Traceroute Setup window 158
Screenshot 153 – The SNMP Audit tool 159
Screenshot 154 - SNMP Walk Setup window 160
Screenshot 155 - Export Configuration settings 161
Screenshot 156 - Import configuration settings 162
Screenshot 157 - Version Information 162
Screenshot 158 – Check for Newer Builds 163
Screenshot 159 - Licensing details 163
Screenshot 160 - VBscript check parameters dialog 166
Screenshot 161 - Add Parameters dialog 167

1 Introduction

1.1 Introduction to GFI Network Server Monitor (GFI NSM)

GFI Network Server Monitor is a network and server monitoring tool that allows administrators to monitor the network for failures or irregularities automatically. With GFI Network Server Monitor, you can identify problems and fix unexpected conditions before your users (or managers) report them to you!

GFI Network Server Monitor maximizes network availability by monitoring all aspects of your servers (including UNIX/LINUX servers), workstations and devices (routers, etc.). When it detects a failure, GFI Network Server Monitor can alert you by email, pager or SMS, as well as take corrective action by, for example, rebooting the computer, restarting a service or running a script or external file. GFI Network Server Monitor can also choose the type of alert to be used, depending on the time that an important event (e.g., check failure) occurs, and also in relation to the working hours you specify during the setup of the intended recipients.

In GFI Network Server Monitor, monitoring checks are created using wizards. A wizard called the Quick Start Wizard, which can create a batch of checks, has also been included. This wizard enables you to quickly create a number of checks at one go - depending on computer OS, role, etc - making it possible for GFI Network Server Monitor to be up and running in the least time possible.

In GFI Network Server Monitor all monitoring checks are organised in folders. You can configure each monitoring check individually or you can choose to configure all the checks in a folder simultaneously through property inheritance. Property Inheritance allows you to set up important check parameters (such as target computer) within the folder properties and have these parameters passed on to the checks contained in that folder.

GFI Network Server Monitor also supports nested folders. This allows for greater flexibility when creating monitoring checks structures that reflect the network layout you are monitoring (by zone, companies being served as well as check function).

1.2 Key features

Enterprise class architecture

GFI Network Server Monitor consists of the monitoring service called the GFI Network Server Monitor 7 Engine, the configuration and management UI program called GFI Network Server Monitor Configuration and a result monitoring service called GFI Network Server Monitor Attendant. No agent software needs to be installed on the computers that you wish to monitor. The Network Monitor Engine is multi-threading and can run 24 checks at a time. This software architecture allows for high reliability and scalability to monitor both large and small networks.

Setup monitor checks using wizards

Check setup wizards help the user to quickly set up an efficient monitoring system using the built-in checks available in just few steps. It is also possible to create a batch of checks simultaneously using the Quick Start Wizard. By default, the Quick Start Wizard can automatically generate monitoring checks for target computers running Windows or specific Linux OSs including SUSE, Mandrake, Redhat and Fedora.

Property inheritance

By default, GFI Network Server Monitor organizes all checks in folders. Through property inheritance, it is possible to specify central properties common to all checks to be contained in a folder (e.g., target computer) and have those properties propagate down to the checks contained in that folder.

Alerts administrators via email, pager or SMS

When it detects a failure, GFI Network Server Monitor can send alerts via SMS/pager, email or a network message. SMS messages are sent through either an SMS service provider (SMSC), directly

through a connected GSM phone/modem or using an Email to SMS service, such as Clickatell. GFI Network Server Monitor can also choose the type of alert to be sent depending on the time that an important event (e.g. check failure) occurs and in relation to the working hours specified for the intended recipients.

In-built Exchange 2000/2003 monitoring

Out of the box, GFI Network Server Monitor checks the status of your Exchange Server by monitoring critical Exchange services and performance counters (Information Store, mailboxes, SMTP service, etc.).

Monitor your database servers (SQL/ODBC)

GFI Network Server Monitor can check for the availability of database applications. Out of the box, it can monitor Microsoft SQL server via ADO. Other databases such as Access, FoxPro, Paradox, SyBase, Informix, IBM DB2 and many more, can be monitored via ODBC.

Monitor remote Event Logs

GFI Network Server Monitor can scan Windows Event logs on local- or remote computers and look for specific Event Sources, Categories, and Event IDs as well as for patterns in the Description of the Event. In addition it can look for multiple events occurring in a specific time interval, for example antivirus alerts posted in the last 30 minutes.

Support for nested folders

Nested folders (folders contained within other folders) are available in the Enterprise/Consultant editions of GFI Network Server Monitor.

Through nested folders, you can organize monitoring checks into a hierarchical structure that reflects specialized monitoring network needs (e.g., grouping of monitoring checks by zone, companies being served, or check type grouping).

Support for SQL Server database backend

Out of the box, the Consultants/Enterprise editions of GFI Network Server Monitor can store monitoring data in MS Access as well as in an SQL Server/MSDE database backend. This new SQL Server support allows you to efficiently monitor and collect network status data from environments which generate large volumes of monitoring data. These include large networks as well as mission-critical systems. You can configure which database backend to use both during installation and after (i.e., from the configuration module).

Built-in checks for computers running Windows OS

- Generic VB Script – Enables you to customize/build monitoring checks using your own VBscript functions.
- OS Object performance counter – Determines the performance of applications by checking the properties of OS objects on target computers.
- Command Line executable output – Executes command line applications and checks text output for specific response.
- Process Properties function – Checks the properties of processes running on target computers (e.g. Memory/CPU/Handles).
- Event Log function – Verifies if the specified (Windows) events, occurred on target computer(s).
- File existence function – Checks for the existence of a particular file; e.g. results of scheduled batch jobs.
- Disk space function – Checks for available/used disk space.
- Services function – Checks if the specified Services are running on local or remote computer.
- CPU usage function – Monitors and restricts processor usage.

- Directory size function – Monitors and restricts the size of a specified directory.
- File size function – Monitors and restricts the size of specified files.
- LDAP Query – Checks the status of LDAP services on target computers.
- Physical Disk Condition function –Checks the physical health of disk drives on windows based target computers.
- Disk drive function - Monitors the physical status of specified disk drives.
- Printer availability function – Checks for the status of printers connected to target computers.
- Process running function – Checks that processes are running on specified target computers.
- Users and Groups Membership function – Monitors user groups against the presence of unauthorized users.

Built-in checks for Windows applications

- Generic ISA Server check – Monitors the status of ISA Server services.
- Generic Exchange Server check – Monitors the status of Exchange services and important performance counters.
- Generic MS SQL/ADO check – Monitors the status of MS SQL databases using ADO.

Built-in checks for databases

- ODBC function – Checks the availability of a database using ODBC.

Built-in checks for network/Internet protocols and services

- HTTP function – Checks the availability of HTTP and Https sites.
- FTP function – Checks the availability of an FTP server/site.
- IMAP function – Checks the availability of IMAP mail servers by remotely connecting to the IMAP port. It can also (optionally) check mailbox authentication as well as count the number of emails in a specific mail folder.
- NNTP news server function - Checks the availability of NNTP news services.
- POP3 server function - Checks POP3 servers by establishing a connection, doing a handshake and optionally authenticate and check the inbox mail count.
- SMTP server function - Monitors mail servers by establishing a connection and doing a handshake in order to check if the SMTP protocol is working correctly. The SMTP check also allows mailbox authentication as well as sending of test emails.
- Terminal services: Port check - Checks if the terminal port is open on local and remote servers.
- NTP timeserver function – Monitors the status of timeservers.
- DNS server function - Checks various types of DNS server records by retrieving record values and comparing them against specified values.
- ICMP ping function - Checks a remote host for availability.
- Generic TCP/IP port function – Checks if a port availability and response.
- Email route function – Checks that the email services are working properly by sending a test email through an SMTP server and verifying that it has been delivered to the destination mailbox.

Built-in checks for SNMP (Simple Network Management Protocol)

- SNMP function – Monitors specified variables on remote computers or devices via the SNMP GET message.

Built-in checks for Linux/Unix OS

- Generic Secure Shell (SSH) check – Allows you to create custom monitor functions which can be remotely executed on Unix/Linux based computers through the Secure Shell (SSH) service running on that computer.
- File existence function – Checks for the existence of a particular file on Linux/Unix based computers; e.g. results of scheduled batch jobs.
- CPU usage function – Checks and restricts processor usage on Linux/Unix based target computers.
- Directory size function – Checks and restricts the size of a specified directory on Linux/Unix based target computers.
- File size function – Checks and restricts the size of a specified file on Linux/Unix based target computers.
- Printer availability function – Checks the status of network printers connected to Linux/Unix based target computers.
- Process running function – Checks if a specified process is running on Linux/Unix based target computers.
- Users and Groups Membership function – Monitors user groups on Linux/Unix based target computers against unauthorized users.
- Disk Partition Check – Checks the state of mounted drives on Linux/Unix based target computers.
- Disk space function – Checks and restricts the available hard disk space on Linux/Unix based target computers.
- Daemons function – Checks the state of a particular daemon on target computers running a Linux/Unix OS.

Take corrective action automatically

When an important event (e.g., check failure) occurs, GFI Network Server Monitor can attempt to correct a problem by restarting a failed service, reboot a target computer/server or launch an executable, batch or VBScript file.

Monitor processes, services & CPU usage

GFI Network Server Monitor enables you to check for critical processes and services running on local and remote computers. You can also monitor the CPU usage of a computer to ensure that applications are running properly.

Build custom network monitor checks using scripts

Although GFI Network Server Monitor includes an extensive set of default monitoring functions, you can build your own custom checks using a scripting language such as VBscript or shell scripts for Unix environments. SSH (Secure Shell) is used for remote connections to Unix based computers. In VBscript, you can make use of WMI and ADSI. WMI is an interface to a broad range of hardware/software/OS-related properties of a computer, allowing you to perform almost any check. Using ADSI you can interface to Active Directory. GFI Network Server Monitor includes a library of sample scripts, and others are continuously being added to the GFI website.

Monitor users, groups & other Active Directory information

Use GFI Network Server Monitor to monitor directory information. For example, monitor group membership of the domain admins group. You can also check user accounts (locked out, disabled, etc.), computer accounts, groups, group membership, organizational units, and so on. A subset of NTDS (NT4-based SAM account database) can be queried too.

Additional Network Support Tools

Additional Network support tools have been included in GFI Network Server Monitor to help you troubleshoot your network. These tools include:-

- Enumerate Computers function – Searches your network for a list of domains, workgroups and constituent computers.
- Enumerate Processes function – Searches for processes running on local or remote computers.
- DNS Lookup function – Resolves Domain Names to their corresponding IP address.
- Whois function – Looks for information related to a specified domain, or IP address.
- Traceroute function – Shows the network path that GFI Network Server Monitor used to reach a target computer.
- SNMP Audit – Performs an SNMP Audit in order to define weak strings.
- SNMP Walk – Allows you to receive SNMP information from an SNMP Server.

Reporting

GFI Network Server Monitor allows you to create reports that detail the availability of your network resources. Such reports can be created in HTML as well as in XML/CSV if they need to be imported by other favorite applications.

Other features

- Allows you to specify maintenance periods to avoid alerts being sent during scheduled maintenance.
- Allows you to store check logs to text file.
- Allows you to setup dependencies to avoid receiving multiple alerts when the servers or services on which other computers depend, are down or unavailable.

1.3 GFI Network Server Monitor components

GFI Network Server Monitor is a client/server application, based on a central monitoring service able to run on Windows NT or higher. This application monitors servers and workstations in your LAN, WAN or even outside your enterprise without the need of any other additional software. This software architecture allows for high reliability and scalability to monitor both large and small networks.

GFI Network Server Monitor consists of 3 main modules which are:-

- NSMUI.exe – Network Server Monitor configuration and user interface.
- NSMENGINE.exe – Network Server Monitor engine/service (multi-threading engine able to run 24 checks at a time).
- NSMATTENDANT.exe – Service which controls web result monitoring, web server access, etc.

1.3.1 Network Server Monitor Engine

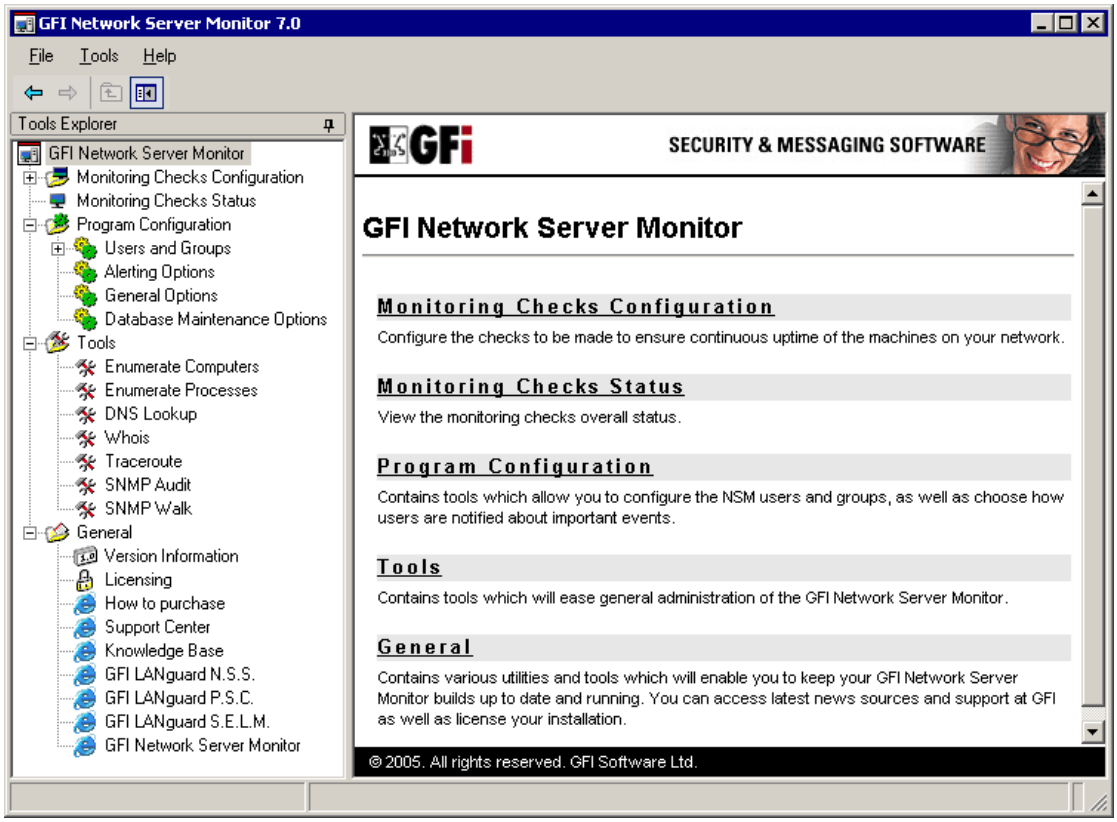
The GFI Network Server Monitor Engine is a windows service that polls the servers in your LAN/WAN for availability at specific time intervals. This is a multithreading service, allowing 24 simultaneous checks to take place at the same time.

GFI Network Server Monitor only makes use of the protocols and application layers available in the Operating System for running its checks, thus no agent software installation is required on the servers to be monitored.

1.3.2 Network Server Monitor configuration

The GFI Network Server Monitor configuration program is the user interface to the GFI Network Server Monitor engine. Use this module to configure all settings required for GFI Network Server

Monitor. To launch this module go on Start > GFI Network Server Monitor program group > GFI Network Server Monitor configuration.


GFI Network Server Monitor 7.0
File Tools Help
Tools Explorer
GFI Network Server Monitor
Monitoring Checks Configuration
Monitoring Checks Status
Program Configuration
Users and Groups
Alerting Options
General Options
Database Maintenance Options
Tools
Enumerate Computers
Enumerate Processes
DNS Lookup
Whois
Traceroute
SNMP Audit
SNMP Walk
General
Version Information
Licensing
How to purchase
Support Center
Knowledge Base
GFI LANguard N.S.S.
GFI LANguard P.S.C.
GFI LANguard S.E.L.M.
GFI Network Server Monitor
GFI
SECURITY & MESSAGING SOFTWARE
GFI Network Server Monitor
Monitoring Checks Configuration
Configure the checks to be made to ensure continuous uptime of the machines on your network.
Monitoring Checks Status
View the monitoring checks overall status.
Program Configuration
Contains tools which allow you to configure the NSM users and groups, as well as choose how users are notified about important events.
Tools
Contains tools which will ease general administration of the GFI Network Server Monitor.
General
Contains various utilities and tools which will enable you to keep your GFI Network Server Monitor builds up to date and running. You can access latest news sources and support at GFI as well as license your installation.
© 2005. All rights reserved. GFI Software Ltd.

Screenshot 1 - The GFI Network Server Monitor configuration

The main GFI Network Server Monitor configuration display is divided into two windows.

- Tools Explorer window (left view) – Contains nodes, check folders and tools required for the configuration and running of GFI Network Server Monitor.
- Event Window (right view) – Multipurpose window in which the contents and options related to the nodes selected in the Tools explorer (left) window are displayed (e.g., Clicking on 'Monitoring Check Status' node in the Tools Explorer, will display the status of monitoring checks in this window).

The GFI Network Server Monitor configuration module can be installed on any local or remote workstation/server running Windows 2000 or higher. GFI Network Server Monitor configuration connects to the GFI Network Server Monitor engine for retrieval of monitoring data.

1.3.3 Network Server Monitor Attendant

The GFI Network Server Monitor attendant module is the service responsible for web result updates and the NSM web server.

1.4 License scheme

The evaluation period allows you to explore and use all features present in GFI Network Server Monitor.

You can purchase a license key online from GFI and use this key without the need to re-install GFI Network Server Monitor. More information on how to order a license key is available at http://www.gfi.com/pricing/pricelist.aspx?product=NSM.

2 Installing GFI Network Server Monitor

2.1 System requirements

2.1.1 Supported operating systems(x86 or x64)

- Windows 2008 (R1 and R2) – Standard, Enterprise
- Windows 2003 – Standard, Enterprise
- Windows 2000 – Professional, Server, Advanced Server
- Windows 7 - Standard, Professional, Enterprise
- Windows Vista – Enterprise, Business, Ultimate
- Windows XP – Professional
- SBS 2008
- SBS 2003

2.1.2 Other components

- Internet Explorer 5.5 (SP2) or later
- .NET framework 1.1
- MDAC 2.6

2.1.3 Target computer components

- WMI – included in Windows 2000 or higher. WMI must be enabled.
- Windows Scripting Host 5.5 or higher – required only if there are configured checks that are using VB Script. Windows Scripting Host is included in Internet Explorer 5.5 (SP2) or higher.

2.1.4 Hardware

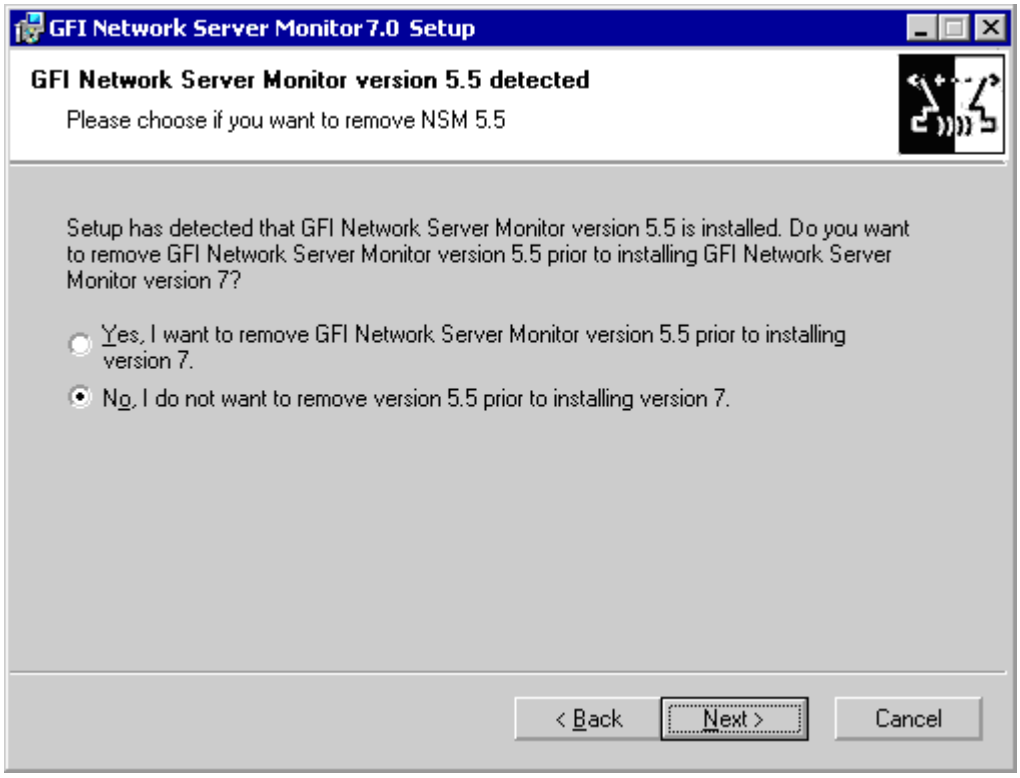
- CPU - 2GHZ
- RAM (minimum/recommended) – 512 MB / 1 GB
- Hard Disk space – 100 Mb

2.2 Installation procedure

The installation wizard installs the actual monitor service, the configuration module and all the required application files automatically. To start an installation:

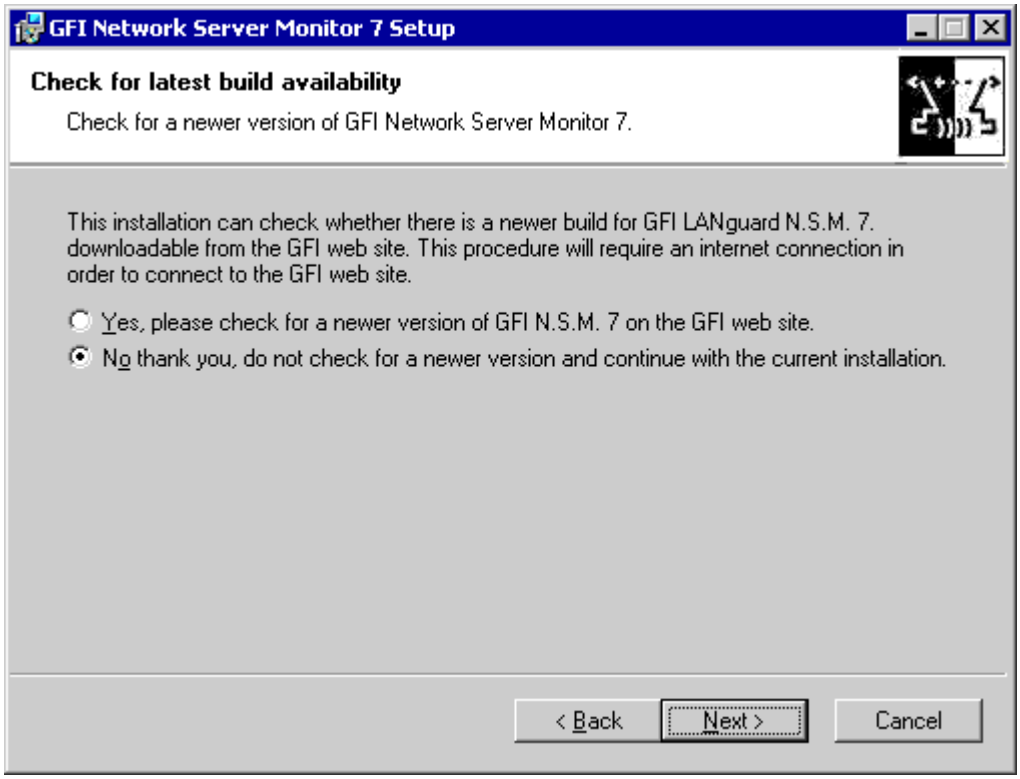
1. Exit all Windows Programs and log on as Administrator.

2. Launch the GFI Network Server Monitor installation wizard by double-clicking on 'NetworkServerMonitor7.exe'. As soon as the welcome dialog is displayed, click on 'Next' to start the installation.


GFI Network Server Monitor 7.0 Setup
GFI Network Server Monitor version 5.5 detected
Please choose if you want to remove NSM 5.5
Setup has detected that GFI Network Server Monitor version 5.5 is installed. Do you want to remove GFI Network Server Monitor version 5.5 prior to installing GFI Network Server Monitor version 7?
Yes, I want to remove GFI Network Server Monitor version 5.5 prior to installing version 7.
No, I do not want to remove version 5.5 prior to installing version 7.
< Back
Next >
Cancel

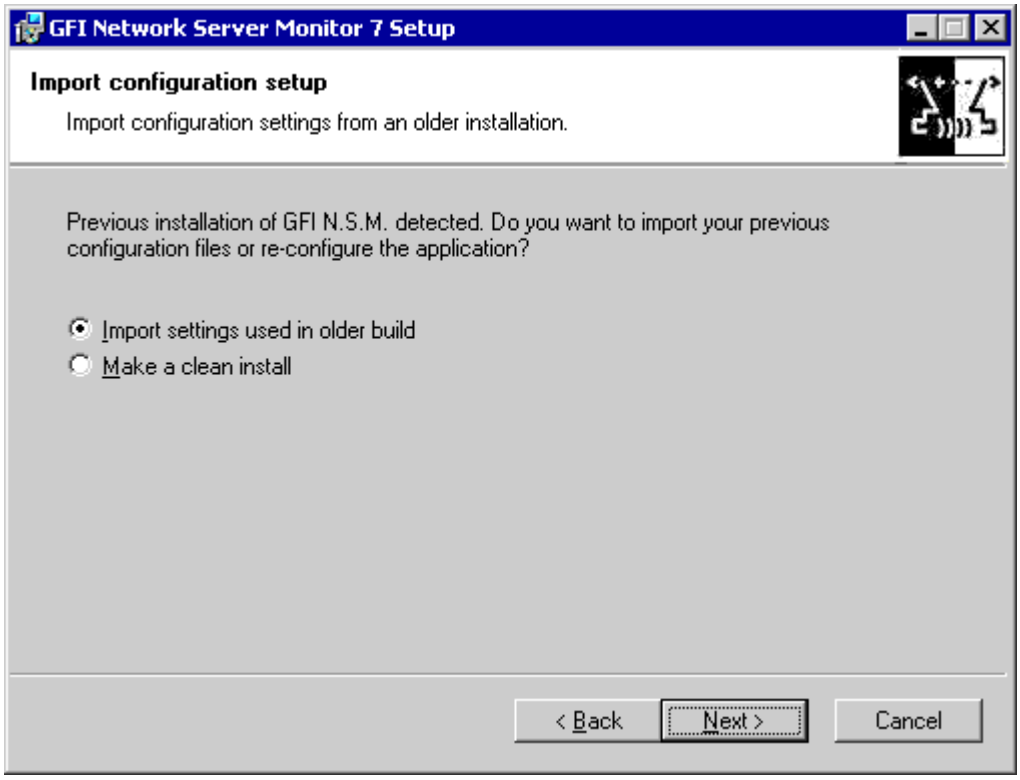
Screenshot 2 - Previous Version Detected

3. The Installation Wizard starts by checking if you have previous versions of GFI Network Server Monitor installed on your computer. Specify if you want to keep any previous installation detected or instruct the wizard to uninstall it for you.


GFI Network Server Monitor 7 Setup
Check for latest build availability
Check for a newer version of GFI Network Server Monitor 7.
This installation can check whether there is a newer build for GFI LANguard N.S.M. 7. downloadable from the GFI web site. This procedure will require an internet connection in order to connect to the GFI web site.
Yes, please check for a newer version of GFI N.S.M. 7 on the GFI web site.
No thank you, do not check for a newer version and continue with the current installation.
< Back
Next >
Cancel

Screenshot 3 - Check for latest build

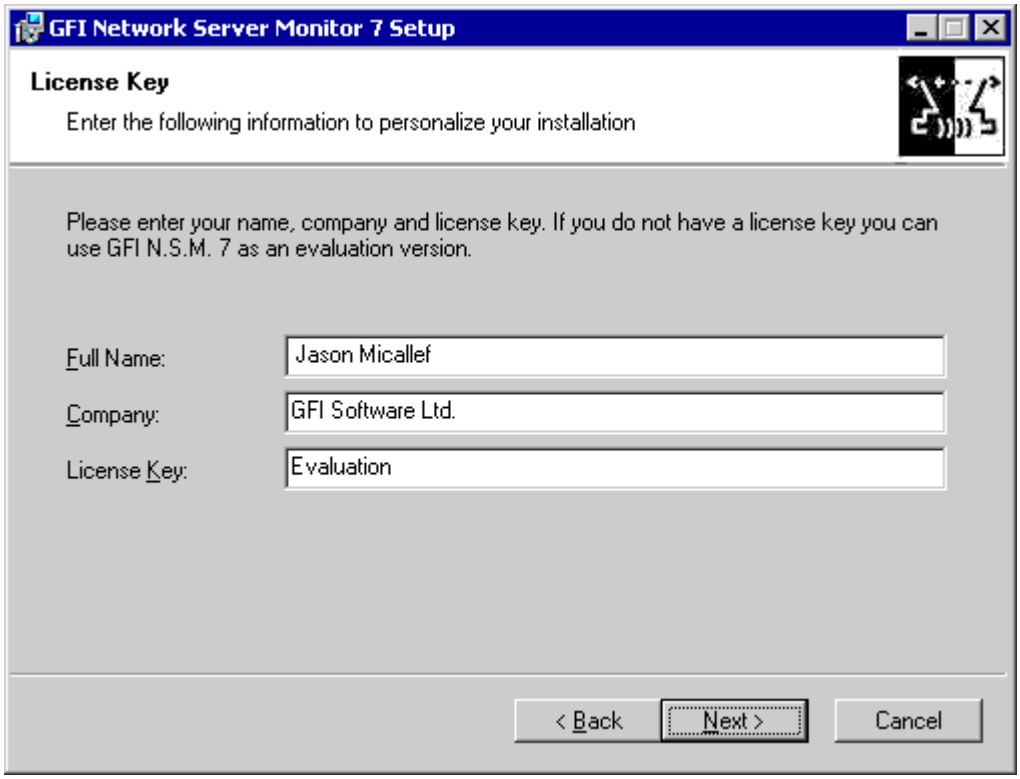
4. Choose whether you want the installation wizard to look for a newer version of GFI Network Server Monitor on the GFI website or click 'Next' to continue with the current installation. In the license dialog, read the licensing agreement carefully. Mark '*I Accept the Licensing agreement*' and click on 'Next' to continue.


GFI Network Server Monitor 7 Setup
Import configuration setup
Import configuration settings from an older installation.
Previous installation of GFI N.S.M. detected. Do you want to import your previous configuration files or re-configure the application?
Import settings used in older build
Make a clean install
< Back
Next >
Cancel

Screenshot 4 - Import settings from an older installation

The following stage is required only if GFI Network Server Monitor 6 or higher have been previously installed on your computer.

5. Choose whether you want to import configuration settings from an existing installation or else continue with a new (clean) installation. Click on 'Next' to continue.

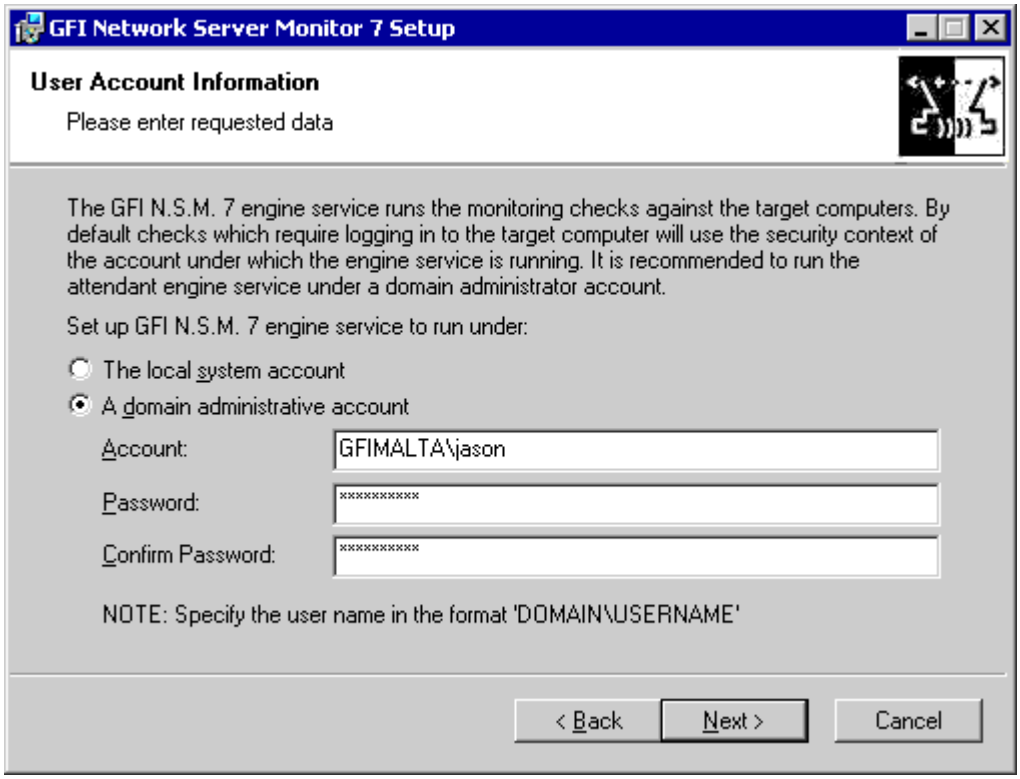

GFI Network Server Monitor 7 Setup
License Key
Enter the following information to personalize your installation
Please enter your name, company and license key. If you do not have a license key you can use GFI N.S.M. 7 as an evaluation version.
Full Name:
Jason Micallef
Company:
GFI Software Ltd.
License Key:
Evaluation
< Back
Next >
Cancel

Screenshot 5 - User and License key details

The following stage is only required during a new (clean) installation.

6. Specify the full user name, the company name and the license key. If you are evaluating the product, leave the evaluation key as default (i.e. “Evaluation”). Click on ‘Next’ to continue.

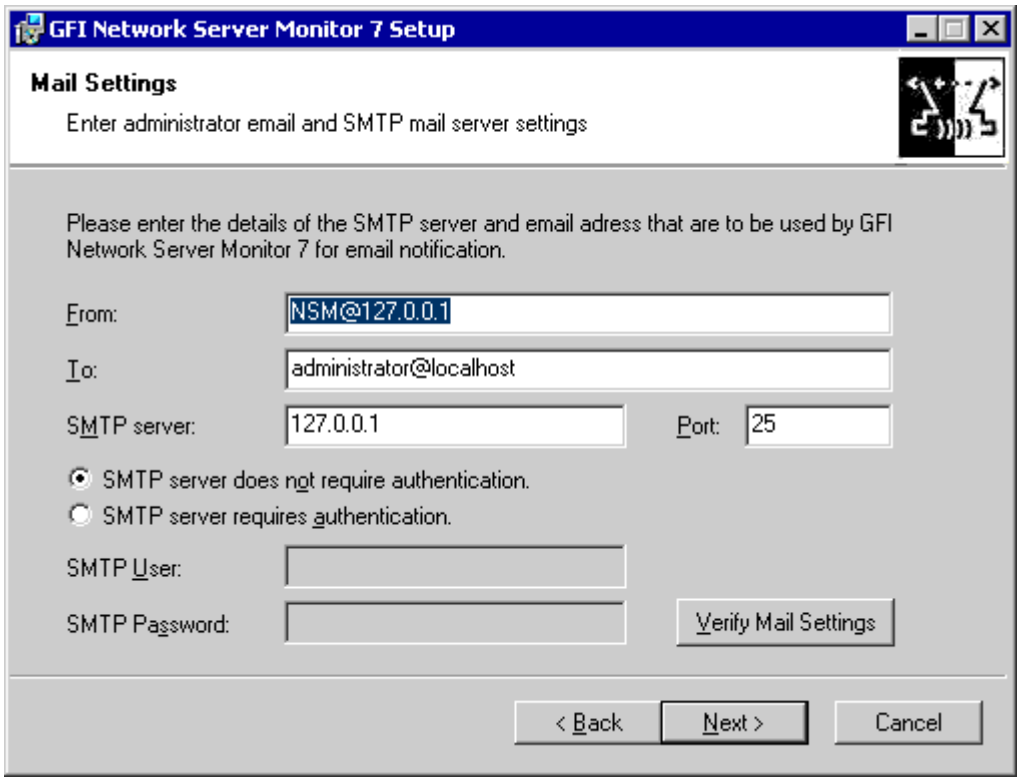
After you have purchased the product, there is no need to uninstall and reconfigure GFI Network Server Monitor because you can enter the new license key directly from the GFI Network Server Monitor configuration program. For more information, please refer to the ‘Entering your License key after installation’ section in this chapter.


GFI Network Server Monitor 7 Setup
User Account Information
Please enter requested data
The GFI N.S.M. 7 engine service runs the monitoring checks against the target computers. By default checks which require logging in to the target computer will use the security context of the account under which the engine service is running. It is recommended to run the attendant engine service under a domain administrator account.
Set up GFI N.S.M. 7 engine service to run under:
The local system account
A domain administrative account
Account:
GFIMALTA\jason
Password:
Confirm Password:
NOTE: Specify the user name in the format 'DOMAIN\USERNAME'
< Back
Next >
Cancel

Screenshot 6- Service Account details

7. Specify a service account for GFI Network Server Monitor.

The GFI Network Server Monitor service must run with administrator credentials. It is recommended to provide a Domain Admin or Enterprise Admin account, because GFI Network Server Monitor will most likely need administrative rights to access the servers on your domain. However, it is not mandatory to provide a Domain/Enterprise Admin account for every monitoring check, since separate credentials can be provided or inherited.



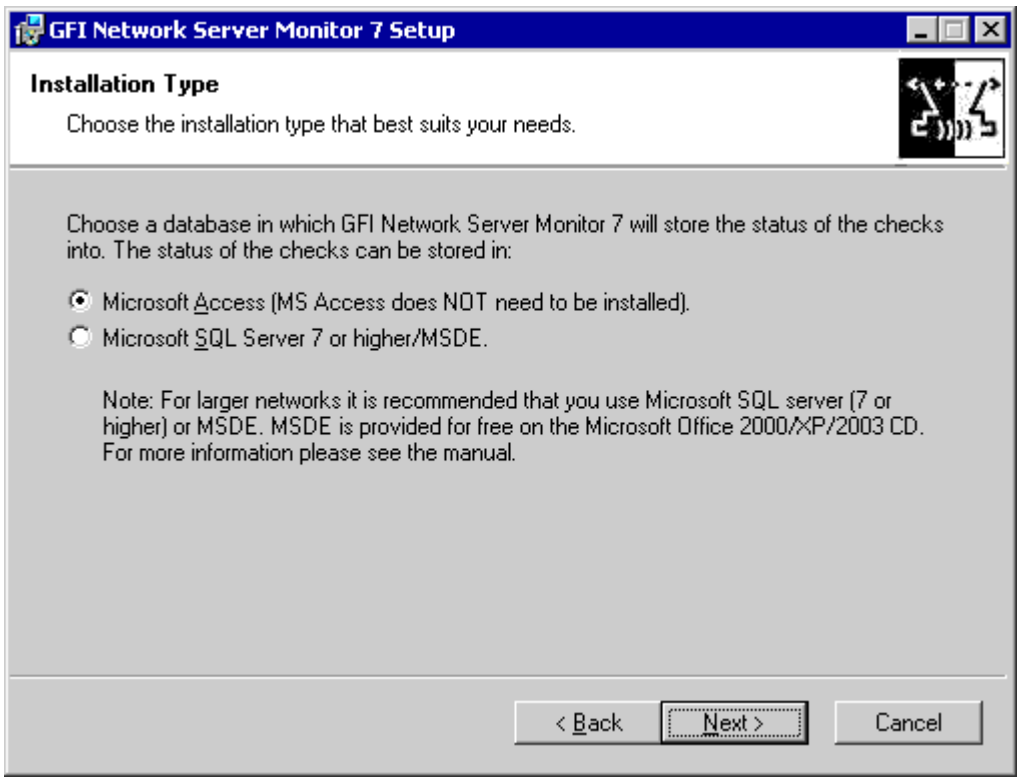
Screenshot 7 - Mail Server details

The following stage is only required during a new (clean) installation.

8. Specify the SMTP/mail server details (Hostname/IP and Port) as well as the email address where generic alerts will be sent. Click on 'Next' to continue.

You can define separate email alert addresses for each check from the check properties during configuration.

You can verify your settings by sending a test message. Do this by clicking on 'Verify Mail Settings'.


GFI Network Server Monitor 7 Setup
Installation Type
Choose the installation type that best suits your needs.
Choose a database in which GFI Network Server Monitor 7 will store the status of the checks into. The status of the checks can be stored in:
Microsoft Access (MS Access does NOT need to be installed).
Microsoft SQL Server 7 or higher/MSDE.
Note: For larger networks it is recommended that you use Microsoft SQL server (7 or higher) or MSDE. MSDE is provided for free on the Microsoft Office 2000/XP/2003 CD. For more information please see the manual.
< Back
Next >
Cancel

Screenshot 8 - Select a database backend

9. Specify which database backend must be used to store the results of its monitoring operations. You can choose between Microsoft Access, Microsoft SQL Server 2000 or MSDE. Click on 'Next' to continue.

MS Access database backend usage is recommended for small networks. For medium and larger networks, usage of Microsoft SQL Server 2000 as a database backend is recommended.

MSDE can handle up to 2GB of data while Microsoft SQL server is capable of handling larger volumes of data efficiently and without limitations.

10. If Microsoft SQL Server is selected as a database backend, specify the IP or hostname on which the SQL server is installed as well as logon credentials. You can use both SQL Server users as well as Windows NT authentication to access the database. Click on 'Next' to continue.

When using Windows NT authentication, ensure that the GFI Network Server Monitor services are running under user accounts which can access the SQL Server databases.

11. Specify the installation path for GFI Network Server Monitor and click on 'Next'. The installation will need approximately 30 MB of free disk space.

12. Click on 'Finish' to finalize the installation and launch GFI Network Server Monitor.

2.3 Entering your license key after installation

If you have purchased GFI Network Server Monitor, launch GFI Network Server Configuration, right click on 'Licensing' in the 'General' node and select 'Enter License key…' Enter the license key in the dialogue on display and click on 'OK'.

By default, GFI Network Server Monitor has an unrestricted fully functional evaluation period of 10 days. If the data you provided in the download form is correct, you will receive by email a license key which enables you to evaluate GFI Network Server Monitor for 30 days.

You must have a GFI Network Server Monitor license for every server that you wish to monitor.

Entering the license key should not be confused with the process of registering your company details on our website. This is important since it allows us to give you support and notify you of important product news. Register on:
http://www.gfi.com/pages/regfrm.htm

2.4 Changing NSM Engine Service logon credentials after installation

The GFI Network Server Monitor Engine Service account details are set up during the installation phase. There is no way to change the service credentials from the GFI Network Server Monitor configuration application. The only way to change such details is as follows:

1. Start >Settings >Control Panel > Administrative Tools >Services.

2. Double click on '*GFI Network Server Monitor 7.0 engine*'.

3. Click on the 'Log On' tab and make the required changes.

4. Click on 'OK' to exit.

3 Configuring GFI Network Server Monitor

3.1 Getting started with GFI Network Server Monitor

All configuration settings for GFI Network Server Monitor are carried out from GFI Network Server Monitor configuration. Launch this configuration program from Start > GFI Network Server Monitor program group > GFI Network Server Monitor configuration.

Introduction to monitor checks

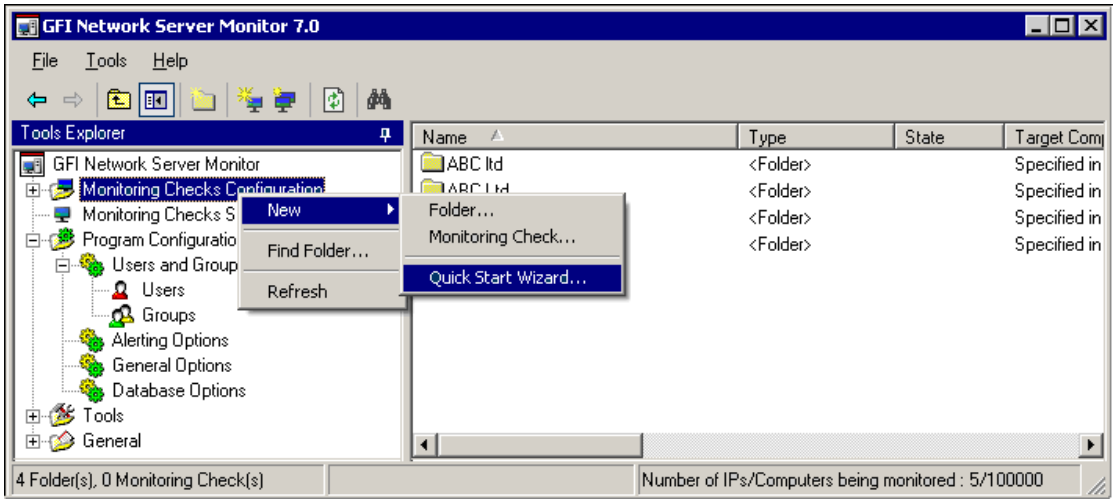
Monitoring checks are tests which verify the condition of specified computers and services on your network. These tests check:

- Hardware status: i.e. verify that target computers and related hardware components are available and running (e.g. Printer availability and Physical disks availability check.)
- Applications and Services: i.e. verify that specific services and applications are running on target computers (e.g. Generic Exchange Server Check and DNS Server checks).

In GFI Network Server Monitor, you can create single checks as well as batches of checks using the available wizards.

3.2 Quick Start Wizard

The Quick Start Wizard helps you quickly create and setup a batch of monitoring checks suitable for your network. This wizard is automatically launched the first time that GFI Network Server Monitor is started, in order to help you get your network monitoring system up and running in the least possible time.

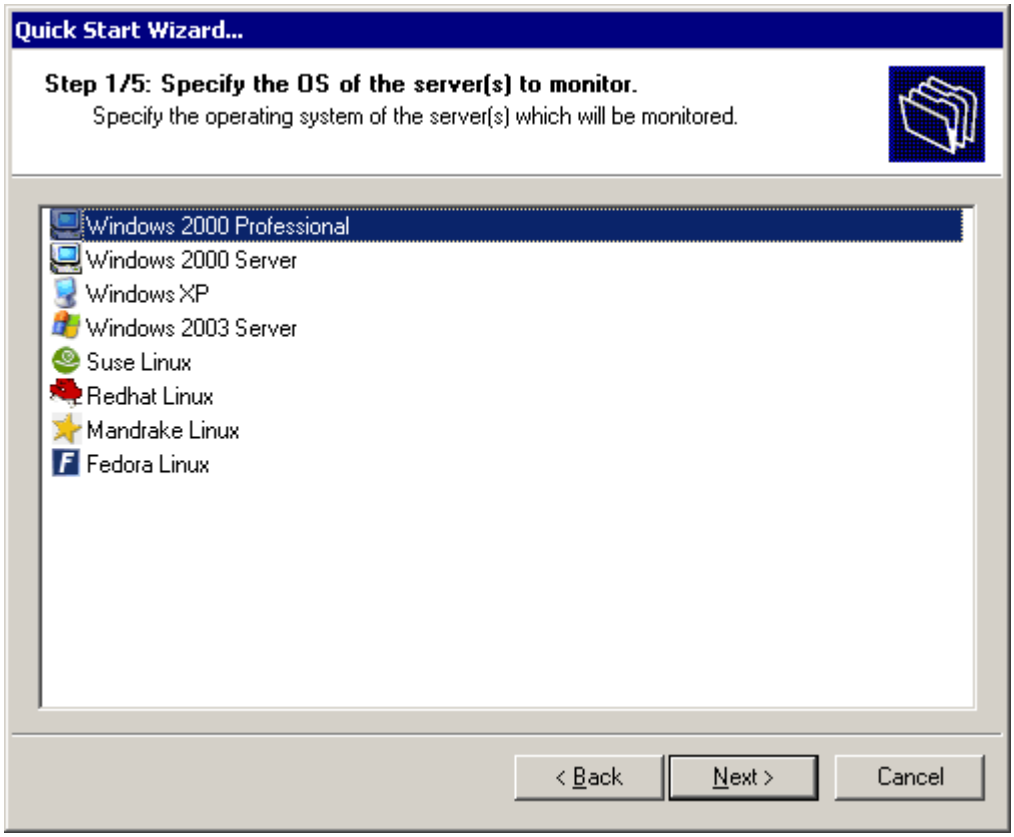


Screenshot 9 - Launching the Quick Start Wizard from the Tools Explorer window

Once ready, you can still make use of this wizard by launching it from File > New > Quick Start Wizard or Right Click on the 'Monitoring Checks Configuration' node in the Tools Explorer window and go to New > 'Quick Start Wizard'.

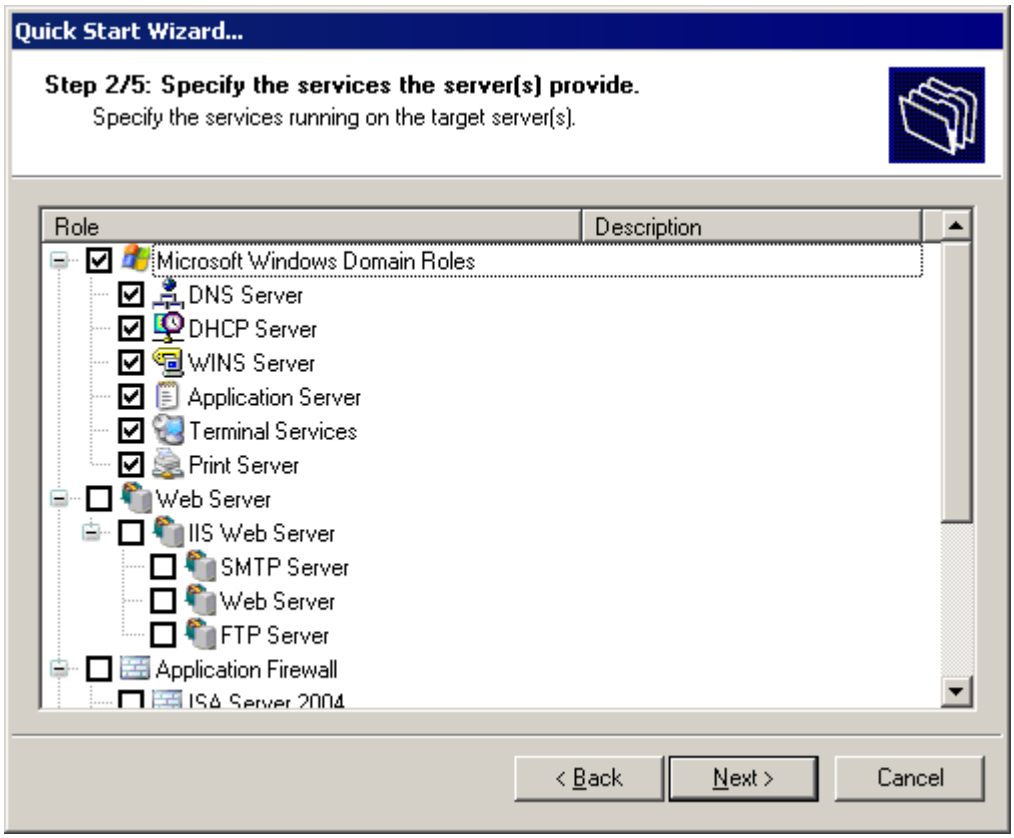
Running the Quick Start Wizard

1. Launch the 'Quick Start Wizard' and click on 'Next'.



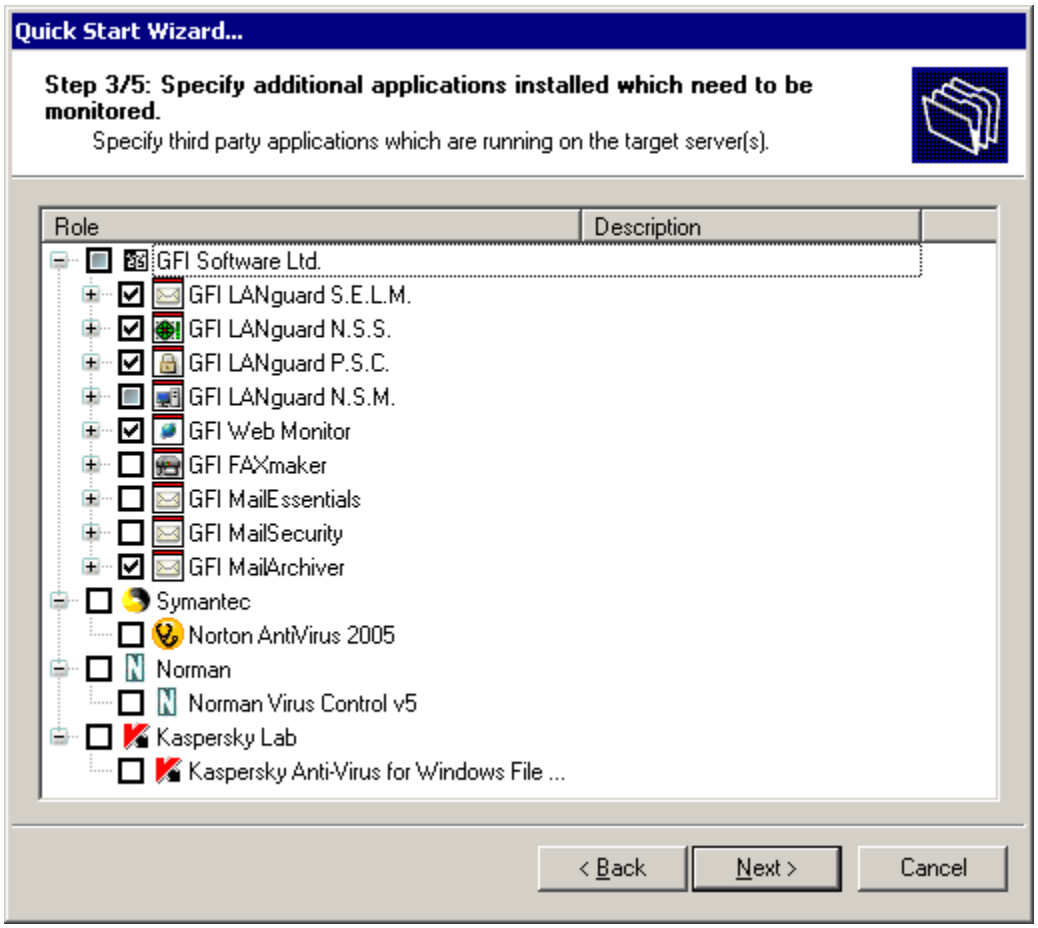
Screenshot 10 - Specify the OS of the target computer

2. Select the operating system installed on your target computer(s).



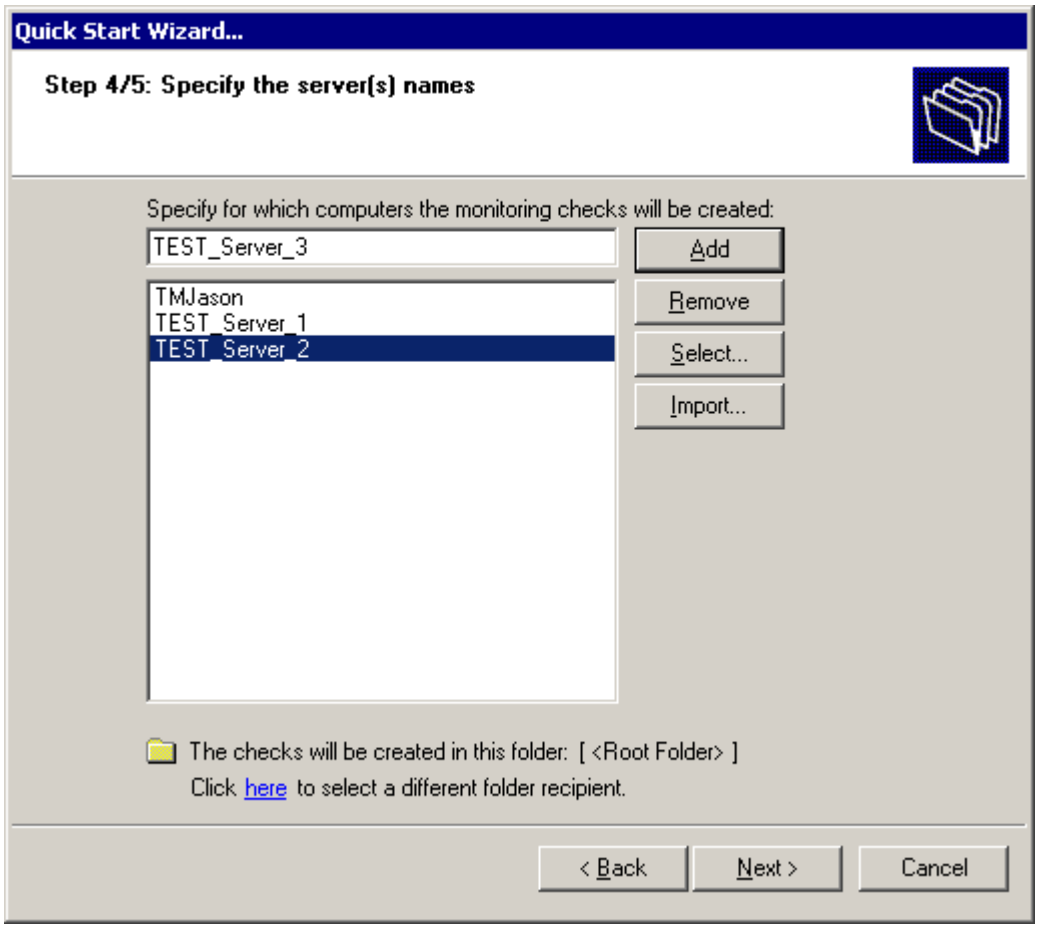
Screenshot 11 - Specify the services provided by the target computer

3. Based on the operating system selection, GFI Network Server Monitor brings up a set of applicable roles for that operating system. Select any additional roles that the target computer(s) have within your network. Click on Next to continue.



Screenshot 12 - Specify additional applications that require monitoring

4. Select any additional important service applications installed on the target computer(s).



Screenshot 13 - Select target computers

5. Specify the target computer(s) on your network which fit the options you selected (operating system / roles / applications). Click on next to continue.

TIP: Use the 'Select' button to choose from a list of computers detected to be running on your network.

TIP: Use the 'Import' button to load the list of target computer name(s) from a text file (plain text file containing one computer name per line).

6. Click on 'Finish'.

A default set of folders (one per target computer) containing the checks for that target computer will be created.

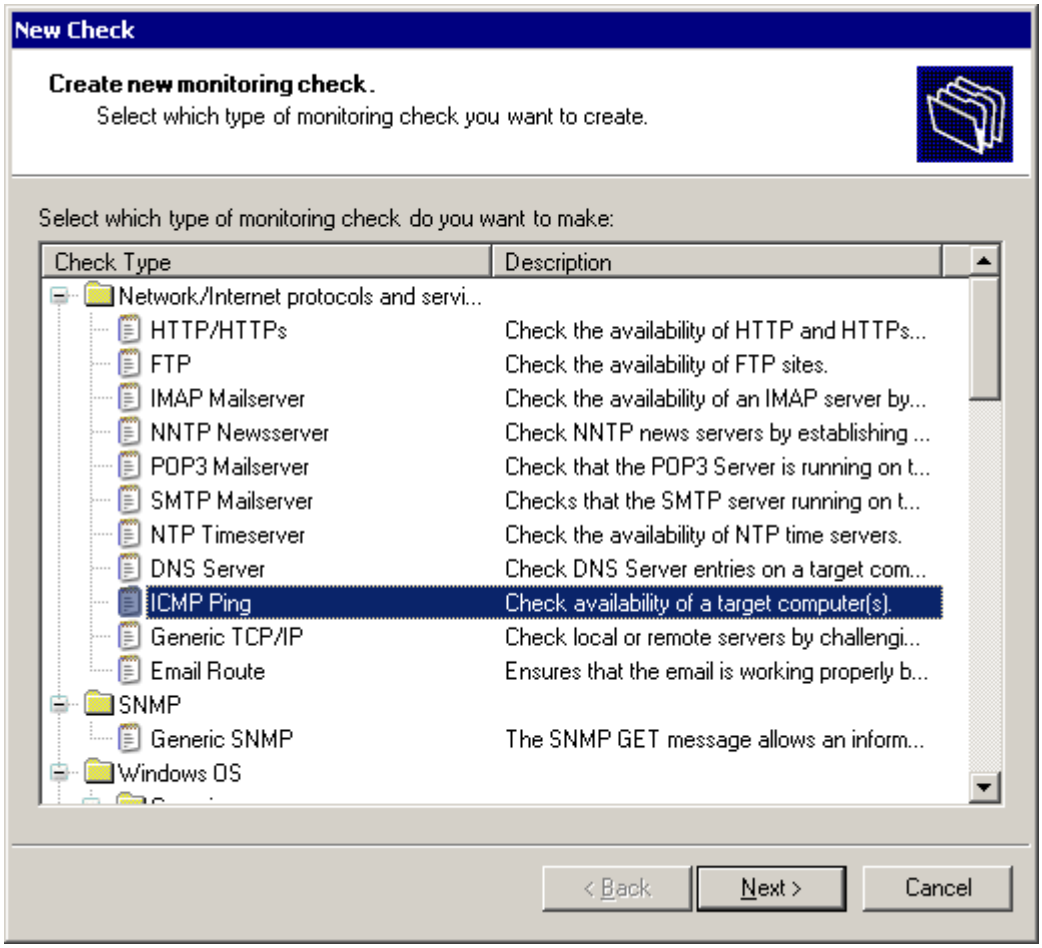
3.3 Creating monitor checks

To generate a new check, use the Create New Monitoring Check Wizard. This wizard asks you for:

- The type of check to create
- The properties relevant for that type of check
- The target(s) to run the monitoring check against.

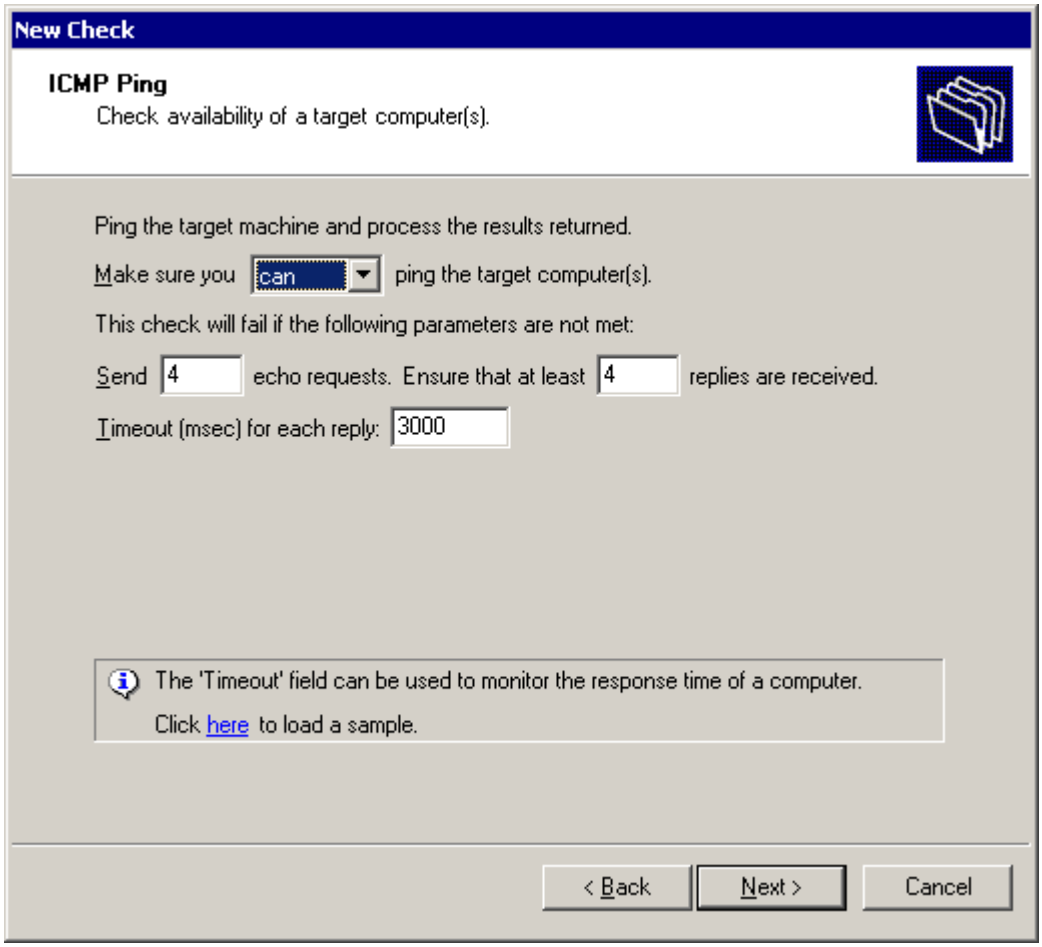
Example: Creating an ICMP Ping check

1. Right-click on the 'Monitoring Checks Configuration' node (in the Tools Explorer (left) window) and go on New > Monitoring Check…


New Check
Create new monitoring check.
Select which type of monitoring check you want to create.
Select which type of monitoring check do you want to make:
Check Type
Description
Network/Internet protocols and servi...
HTTP/HTTPs
Check the availability of HTTP and HTTPs...
FTP
Check the availability of FTP sites.
IMAP Mailserver
Check the availability of an IMAP server by...
NNTP Newsserver
Check NNTP news servers by establishing ...
POP3 Mailserver
Check that the POP3 Server is running on t...
SMTP Mailserver
Checks that the SMTP server running on t...
NTP Timeserver
Check the availability of NTP time servers.
DNS Server
Check DNS Server entries on a target com...
ICMP Ping
Check availability of a target computer(s).
Generic TCP/IP
Check local or remote servers by challengi...
Email Route
Ensures that the email is working properly b...
SNMP
Generic SNMP
The SNMP GET message allows an inform...
Windows OS
< Back
Next >
Cancel

Screenshot 14 - Select Type of Monitoring Check required

2. Select the type of monitoring check to create (e.g., if you want to check the availability of a target computer, select 'ICMP Ping'). Click on 'Next' to continue.

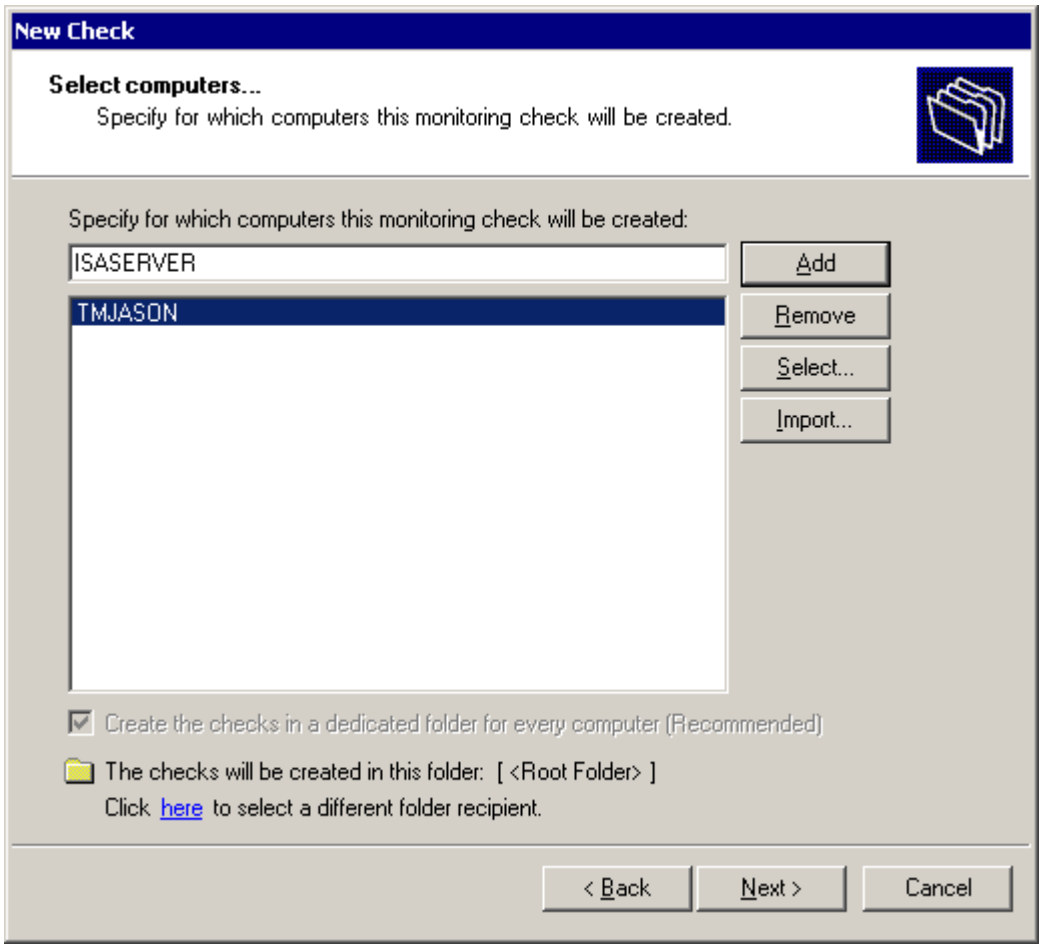

New Check
ICMP Ping
Check availability of a target computer(s).
Ping the target machine and process the results returned.
Make sure you can ping the target computer(s).
This check will fail if the following parameters are not met:
Send 4 echo requests. Ensure that at least 4 replies are received.
Timeout (msec) for each reply: 3000
The 'Timeout' field can be used to monitor the response time of a computer.
Click here to load a sample.
< Back
Next >
Cancel

Screenshot 15 - ICMP/Ping check properties dialog

3. Configure the parameters to be used by the selected check. Click on 'Next' to continue. The ICMP/Ping check requires the following parameters:

- *Make sure you…..ping the target computer* – Specify whether the ping will succeed or fail if a ping reply is received.
- *Number of Echo requests to send* – Specify the number of consecutive pings to be sent (e.g., 4)
- *Minimum number of expected replies* – Specify the minimum number of replies that must be received in order for the check to succeed. (e.g., 4)
- *Timeout (m.sec) for each reply* – Specify the expected response time (in milliseconds). This is the time that the check will wait for a response to an echo request (i.e., the time between successive echo requests).

On a congested network, echo response packets may take longer than 3 seconds to be delivered. To avoid false alarms, adjust the timeout value according to the traffic present on your network.


New Check
Select computers...
Specify for which computers this monitoring check will be created.
Specify for which computers this monitoring check will be created:
ISASERVER
Add
TMJASON
Remove
Select...
Import...
Create the checks in a dedicated folder for every computer (Recommended)
The checks will be created in this folder: [<Root Folder>]
Click here to select a different folder recipient.
< Back
Next >
Cancel

Screenshot 16 - The Select Computer(s) dialog

4. Select the target computer(s) to ping.

TIP 1: You can also enumerate target computers by clicking on 'Select'. This will open a dialog from where you can choose the required target computer(s).

TIP 2: You can import the list of target computers from a text file using the 'Import' button. However make sure that the text file is in plain text.

5. Optionally, you can specify a short description for the new check(s) to be created.

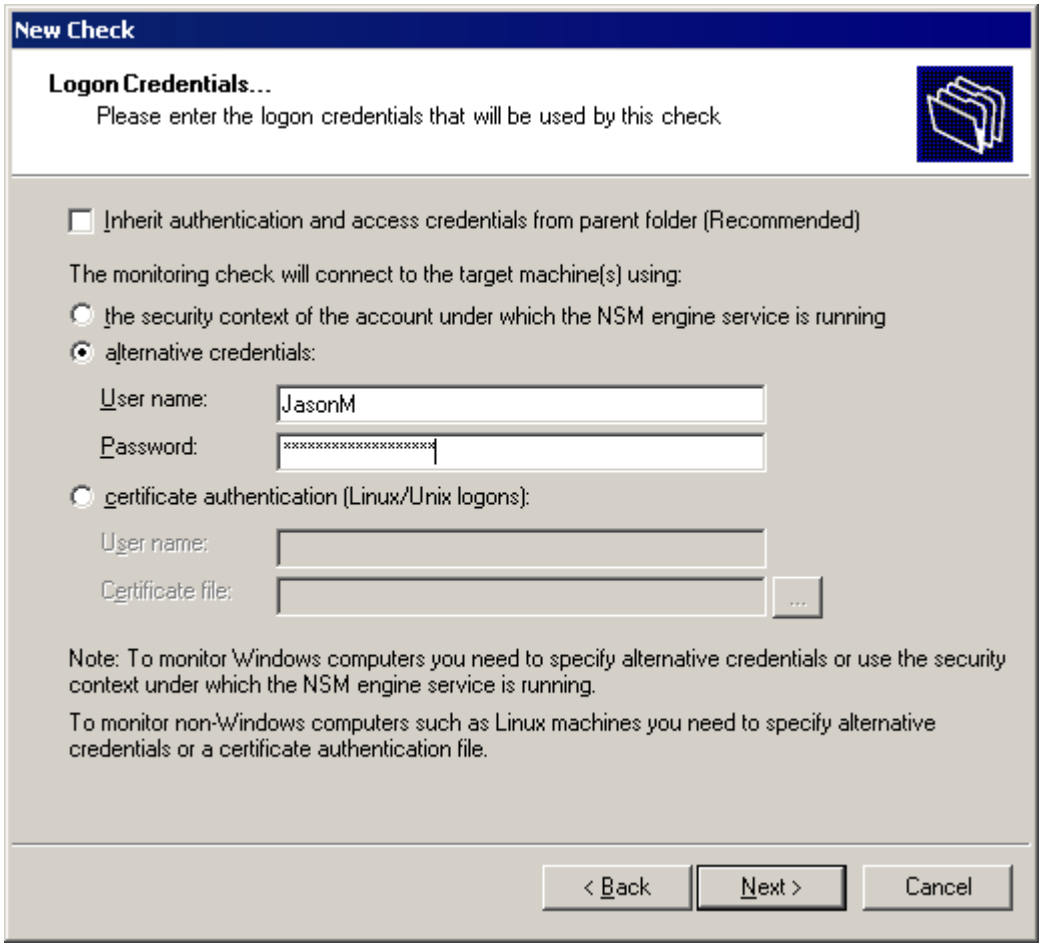
6. Click on 'Finish' to generate the ICMP ping check(s) for the selected target computer(s).

Different types of checks: Different properties

GFI Network Server Monitor ships with a selection of monitoring checks. Different monitoring checks require different parameters to operate. The New Check Wizard asks you to specify the parameters required by the selected check during its creation.

Logon credentials

Some type of checks (e.g., IMAP, POP3) may require alternative logon credentials to the ones used to log on to the target computer. When applicable you will be asked to confirm or specify alternative logon credentials to be used for that check.


New Check
Logon Credentials...
Please enter the logon credentials that will be used by this check
Inherit authentication and access credentials from parent folder (Recommended)
The monitoring check will connect to the target machine(s) using:
the security context of the account under which the NSM engine service is running
alternative credentials:
User name:
JasonM
Password:
certificate authentication (Linux/Unix logons):
User name:
Certificate file:
...
Note: To monitor Windows computers you need to specify alternative credentials or use the security context under which the NSM engine service is running.
To monitor non-Windows computers such as Linux machines you need to specify alternative credentials or a certificate authentication file.
< Back
Next >
Cancel

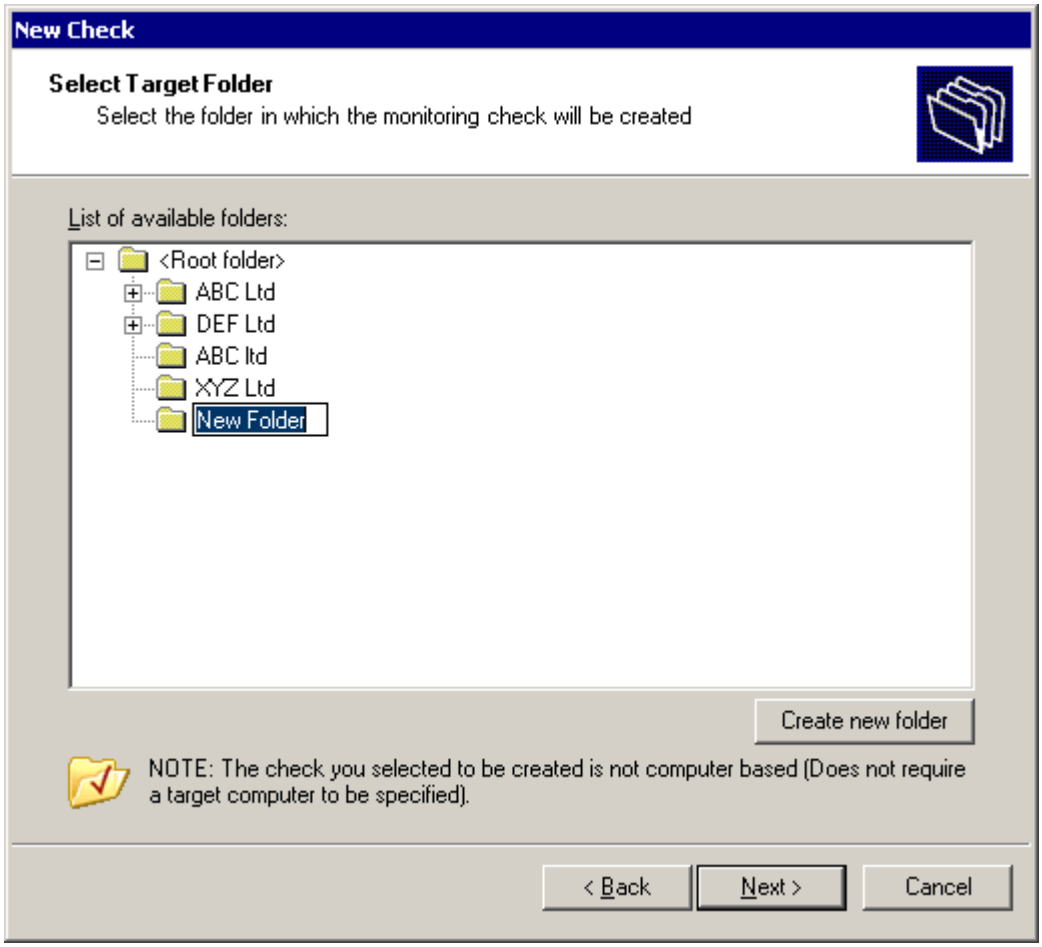
Screenshot 17 - Logon Credentials dialog

As an example, the IMAP Mailserver check uses logon credentials to connect to the mailserver and check its availability. In addition, this check also requires alternative credentials to physically log on to target a mailbox (i.e., perform a mailbox authentication check) in order to count the number of emails in a specific folder within this mailbox.

By default, logon credentials parameters are inherited from the parent folder. To specify alternative credentials (e.g., for mailbox access), unselect the option 'Inherit username and password from parent folder' option and configure accordingly. Click on 'Next' to continue.

Non computer specific checks

Some type of checks (e.g., http/https) are not computer-specific. While the web server may be running on a computer in your domain, when querying a website, you will not specify the target computer but the domain to query. When this is the case, you will be asked to select a folder under which to put the newly created checks.


New Check
Select Target Folder
Select the folder in which the monitoring check will be created
List of available folders:
<Root folder>
ABC Ltd
DEF Ltd
ABC ltd
XYZ Ltd
New Folder
Create new folder
NOTE: The check you selected to be created is not computer based (Does not require a target computer to be specified).
< Back
Next >
Cancel

Screenshot 18 - The Select Target folder dialog

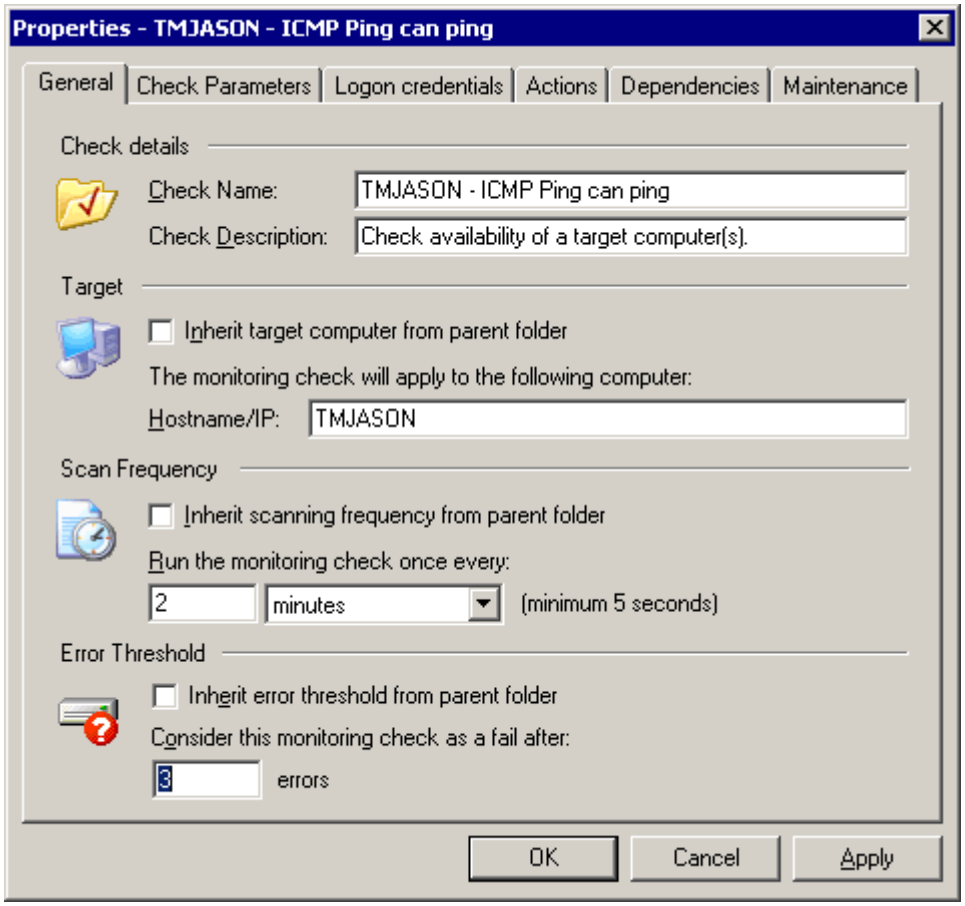
Refer to 'Configuring Monitor Functions' chapter for more information on the type of checks supported by GFI Network Server Monitor.

3.4 Configure monitor check properties

About monitor check properties

Monitoring checks require parameters which define their performance. (E.g. the 'Scan Frequency' defines the time interval between consecutive runs of a monitoring check). These parameters also pre-define the actions that GFI Network Server Monitor must trigger when a check succeeds or fails (e.g. Alert parameters designate the type of alert to be sent, including its recipient(s)). Parameters can be directly configured from the check properties or inherited from the properties of the folder where the checks are stored. For further information on how to inherit properties, please refer to the 'Inherit properties from folders' section in this chapter.

3.4.1 Configure general parameters



Screenshot 19 - Check properties dialog

To specify the general parameters of a monitor check (e.g., Check Name and Target Computer):

1. Right click on the check to be configured and select 'Properties'. By default the check properties dialog will open in the 'General' tab.

2. Specify the following parameters:

- Check details – The monitoring check name (e.g. 'Fileserver Availability Check') and relative function description (e.g. Ping the Fileserver to check if it is available).
- Target – The name or IP address of the target computer on which this check will run (e.g. FILESERVER or 192.168.1.10).
- Scan Frequency – The time interval between consecutive executions of this monitoring check (e.g. Specify a scan frequency of 10 minutes, if you want to run this check every 10 minutes).
- Error Threshold – The number of consecutive times that this check must fail before an action is triggered (e.g. Specify an Error Threshold of 3, to allow a check to fail 3 consecutive times, before the check is classified as failed and alerts, etc. are triggered).

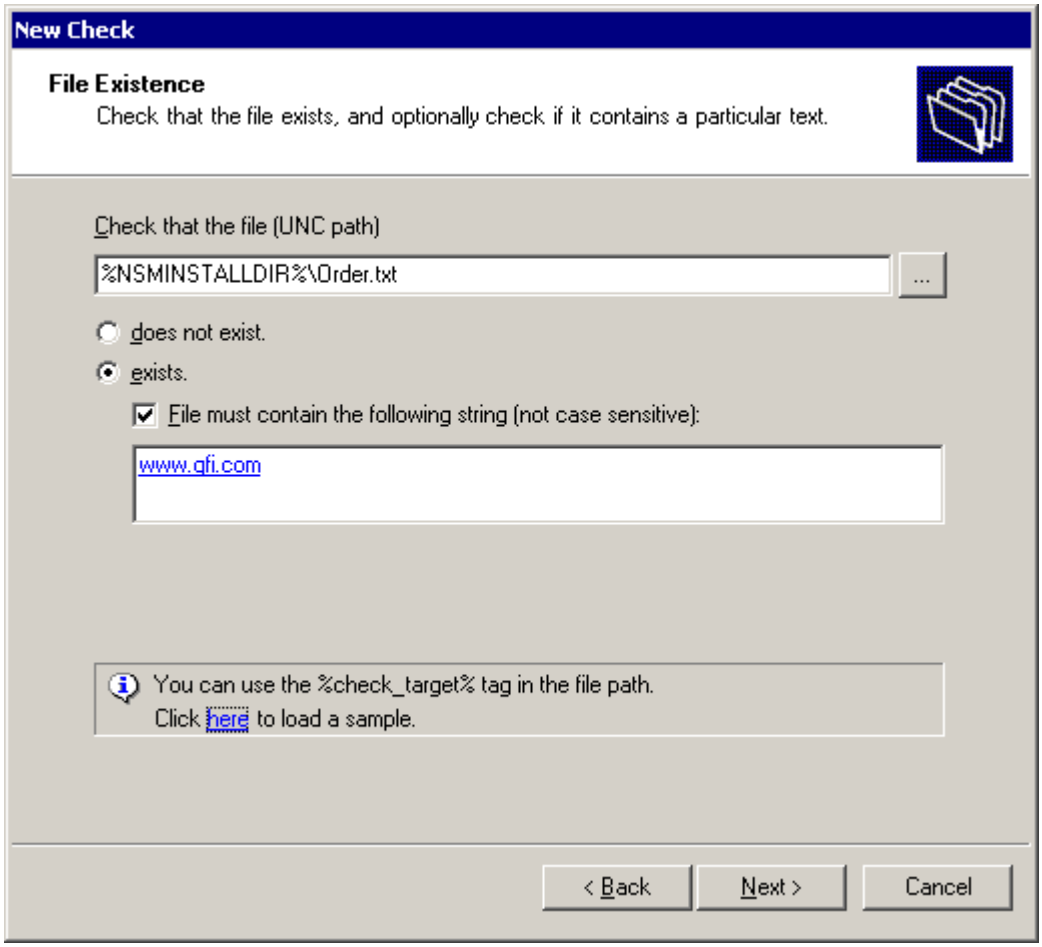
Check failures occurring within the specified error threshold limit are known as errors. GFI Network Server Monitor only defines a check as failed when the number of errors exceeds the error threshold. The error threshold is necessary to avoid continuous false alarms, triggered by check timeouts, associated with slow network connections or delays in connection in extremely busy targets (e.g. File servers and Mail servers) during peak hours.

3.4.2 Configure check (functional) parameters

The check functional parameters are the test settings that define the role of a monitoring check (i.e., each type of monitoring check requires its own configuration settings and parameters). For further information on functional parameter setups, please refer to the Configuring monitor functions chapter in this manual.

Example: Configuring the functional parameters of a File Existence check.

GFI Network Server Monitor can check for the existence of a file. In this example, the monitoring check will be setup to look for a file called 'status.txt'.


New Check
File Existence
Check that the file exists, and optionally check if it contains a particular text.
Check that the file (UNC path)
%NSMINSTALLDIR%\Order.txt
...
does not exist.
exists.
File must contain the following string (not case sensitive):
www.gfi.com
You can use the %check_target% tag in the file path.
Click here to load a sample.
< Back
Next >
Cancel

Screenshot 20 - File existence check parameters

1. Right click on the check to be configured and select 'Properties'. By default the check properties dialog will open in the 'General' tab.

2. Click on the 'Check Parameters' Tab and specify the following parameters:

- File (UNC Path) – The path to the file in UNC format (e.g. \\machine\monitor\status.txt) that needs to be checked.
- Exists - Enable the 'Exist' option to specify that this check must find the specified file to be successful.
- File must contain…. – Enable this option and specify the string that must be present in the file in order for the check to be successful (e.g. 'transfer was successful').

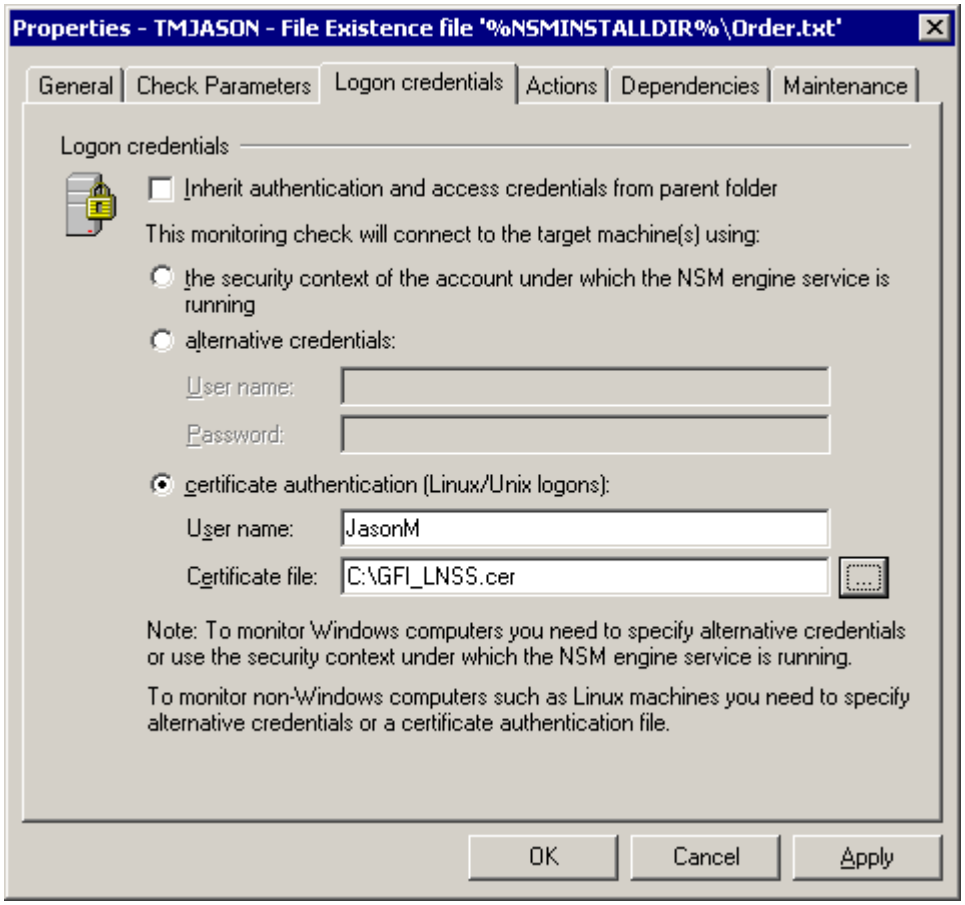
3. Click on 'Apply' to accept the current configuration.

3.4.3 Define logon credentials

The logon credentials are the (logon) authentication details which a monitoring check requires to connect to a target computer.

Computers running on Linux and Unix may require reference to a certificate authentication (private key) file instead of the logon password. The certificate authentication file is often required by the SSH module for authentication by Linux/Unix computers.

By default, GFI Network Server Monitor uses the same security context account used by the GFI Network Server Monitor engine.


Properties - TMJASON - File Existence file '%NSMINSTALLDIR%\Order.txt'
General
Check Parameters
Logon credentials
Actions
Dependencies
Maintenance
Logon credentials
Inherit authentication and access credentials from parent folder
This monitoring check will connect to the target machine(s) using:
the security context of the account under which the NSM engine service is running
alternative credentials:
User name:
Password:
certificate authentication (Linux/Unix logons):
User name:
JasonM
Certificate file:
C:\GFI_LNSS.cer
Note: To monitor Windows computers you need to specify alternative credentials or use the security context under which the NSM engine service is running.
To monitor non-Windows computers such as Linux machines you need to specify alternative credentials or a certificate authentication file.
OK
Cancel
Apply

Screenshot 21 - Logon Credentials Setup Dialog

To setup alternative or certificate authentication credentials:

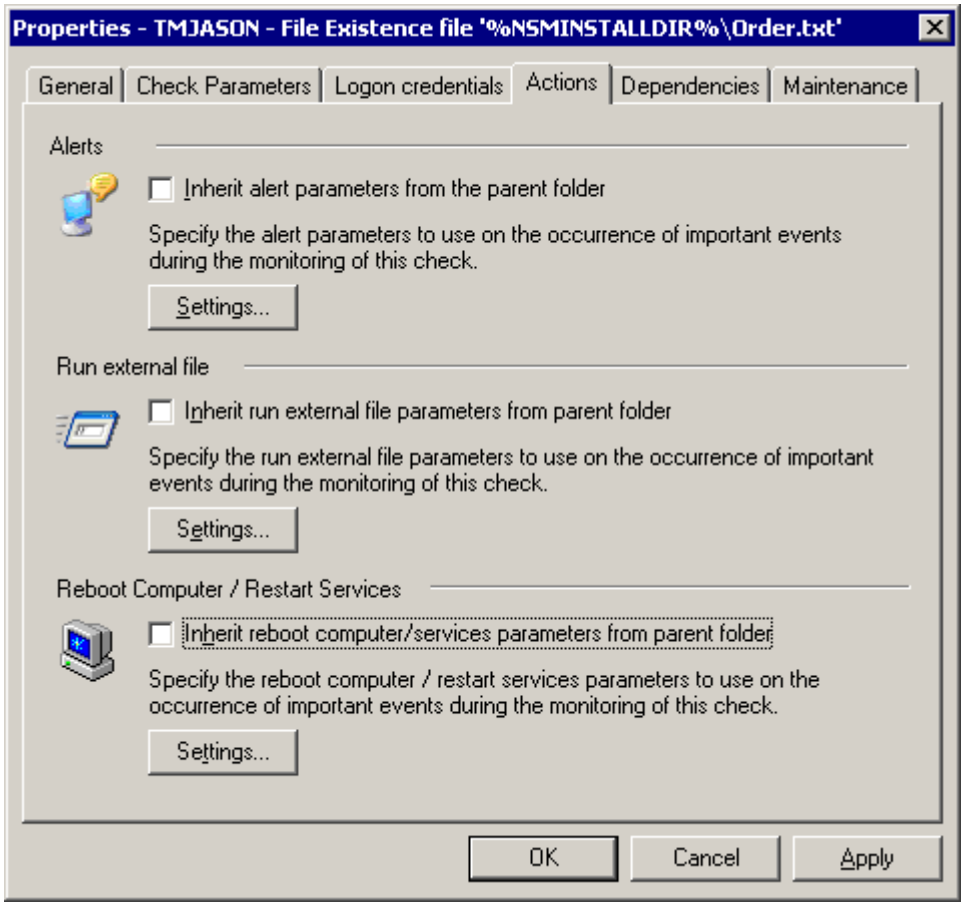
1. Right click on the check to be configured and select 'Properties'. By default the check properties dialog will open in the 'General' tab.

2. Click on the 'Logon Credentials' Tab. If the '*Inherit authentication and access credentials from Parent folder*' option is selected, unselect it and choose the '*Alternative Credentials*' option or the '*Certificate Authentication*' option instead

3. Specify the user name (e.g., JasonM) and the password or the full path to the certificate file (e.g., /etc/passwd/cert_file).

4. When ready, click on 'Apply' to accept the current configuration.

Alerts and actions


Properties - TMJASON - File Existence file '%NSMINSTALLDIR%\Order.txt'
General
Check Parameters
Logon credentials
Actions
Dependencies
Maintenance
Alerts
Inherit alert parameters from the parent folder
Specify the alert parameters to use on the occurrence of important events during the monitoring of this check.
Settings...
Run external file
Inherit run external file parameters from parent folder
Specify the run external file parameters to use on the occurrence of important events during the monitoring of this check.
Settings...
Reboot Computer / Restart Services
Inherit reboot computer/services parameters from parent folder
Specify the reboot computer / restart services parameters to use on the occurrence of important events during the monitoring of this check.
Settings...
OK
Cancel
Apply

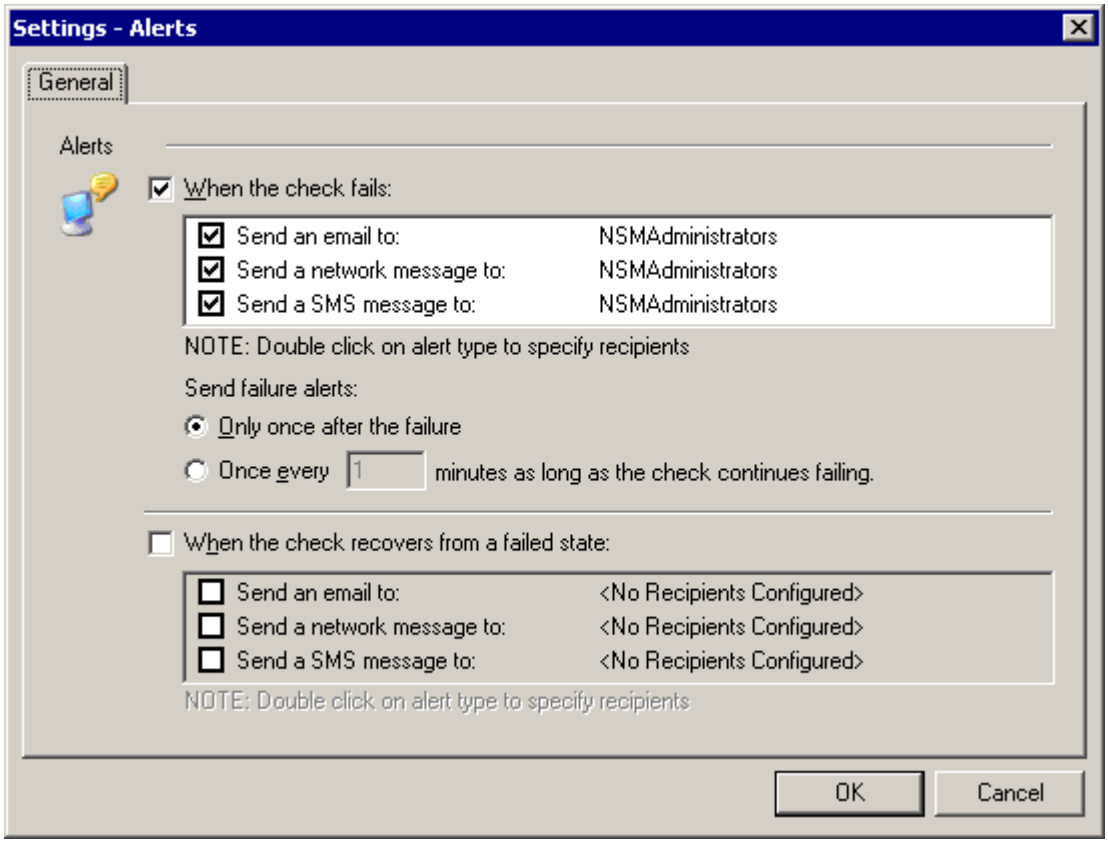
Screenshot 22 - Actions Setup dialog

Actions refer to the activities which follow the occurrence of an important event, i.e., what happens when a monitoring check meets a specified condition. GFI Network Server Monitor supports the following actions:

- Alerts – Send messages to inform the recipient(s) of the event(s).
- Run an external file – Launch an executable, batch or VBScript file when a particular check fails.
- Rebooting a computer – Attempt to automatically correct a problem by rebooting the target computer which has failed.
- Restarting services – Attempt to automatically correct a problem by restarting the service(s) which have failed during a check.

Alerts

GFI Network Server Monitor supports email alerts., network alerts and SMS/pager alerts.



Screenshot 23- Alerts Setup Dialog

These alerts can be sent in two situations:

- When a monitoring check fails – after a configurable number of errors, the monitor check is considered as failed.
- When a monitoring check has recovered from the 'Failed' state – since GFI Network Server Monitor can recover a server/device, it can be useful to send an alert to the operator to inform him/her that the previous error is no longer present.

About email alerts

To use SMTP email alerts, the GFI Network Server Monitor service must have access to an SMTP compliant mail server. GFI Network Server Monitor also supports SMTP servers that require SMTP authentication, such as the Microsoft Exchange\IIS SMTP server. SMTP AUTH is a protocol that is used to verify that you are a user on the SMTP server. GFI Network Server Monitor is RFC 821 and RFC 822 SMTP AUTH compliant.

GFI Network Server Monitor does not require IIS to support e-mail; it communicates directly to the SMTP server using the SMTP protocol.

About network alerts

GFI Network Server Monitor makes use of 'Net Send' (or 'Net Popup') to send messages over the network.

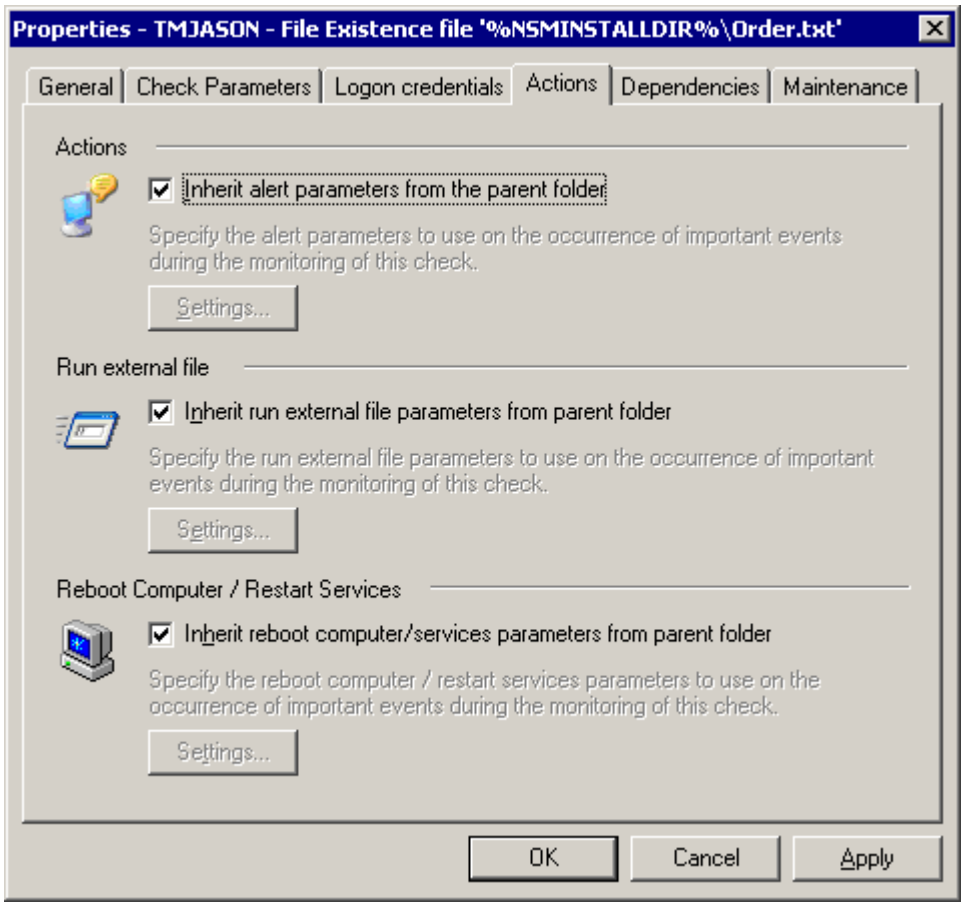
Only computers that support NetBIOS can send and receive network messages. NetBIOS messages can be sent to users and/or computers.

About SMS/pager alerts

GFI Network Server Monitor can send SMS messages through an SMS Center (via an attached modem), directly through an attached GSM device (e.g., cell phone) or via a web-based SMS gateway. When an SMS alert is to be sent through an SMS Center, GFI Network Server Monitor

uses the modem to dial in to the SMSC provider and deliver the actual SMS message(s); most countries have one or more SMSC service providers. When an SMS alert is to be sent via a web-based SMS gateway, GFI Network Server Monitor generates an email containing all the alert details. This email is then sent to the web-based SMS gateway where it is converted to an SMS and forwarded to the intended recipient.

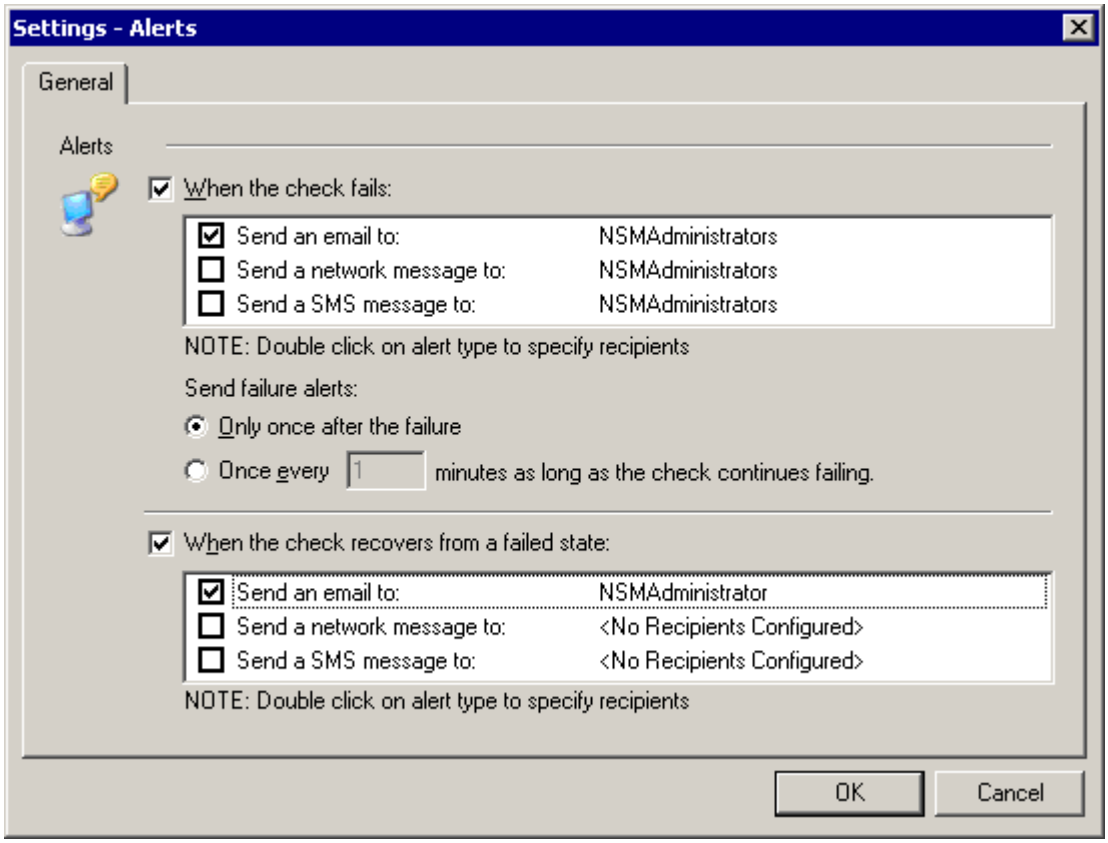
3.4.4 Configure alert parameters


Properties - TMJASON - File Existence file '%NSMINSTALLDIR%\Order.txt'
General
Check Parameters
Logon credentials
Actions
Dependencies
Maintenance
Actions
Inherit alert parameters from the parent folder
Specify the alert parameters to use on the occurrence of important events during the monitoring of this check.
Settings...
Run external file
Inherit run external file parameters from parent folder
Specify the run external file parameters to use on the occurrence of important events during the monitoring of this check.
Settings...
Reboot Computer / Restart Services
Inherit reboot computer/services parameters from parent folder
Specify the reboot computer / restart services parameters to use on the occurrence of important events during the monitoring of this check.
Settings...
OK
Cancel
Apply

Screenshot 24 - Actions dialog with Inherit options enabled

1. Right click on the check to be configured and select 'Properties'. By default the check properties dialog will open in the 'General' tab.

2. Click on the 'Actions' tab. If the '*Inherit alert parameters from the Parent folder*' option is selected (see above screenshot), unselect it and click on 'Settings' in the Alerts area.

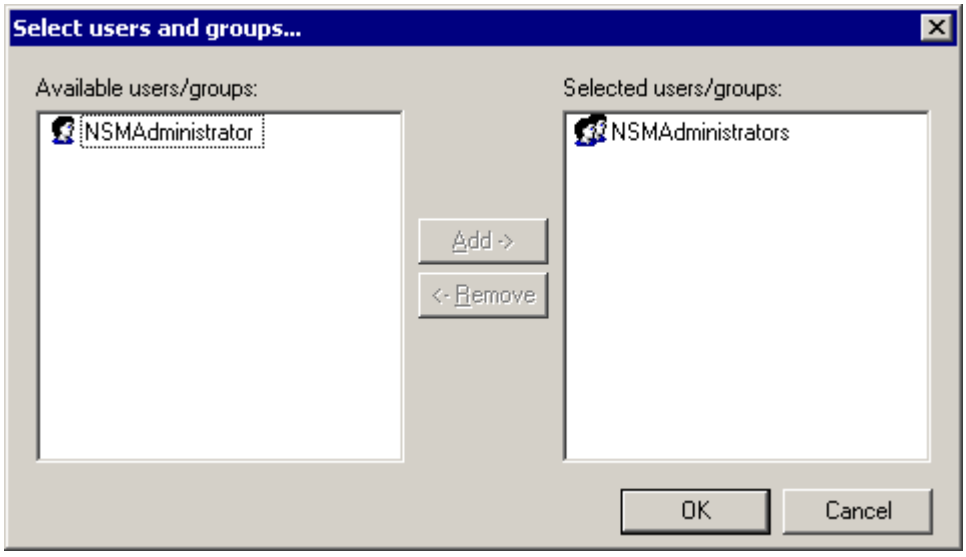


Screenshot 25 - Alerts setup dialog

3. Choose the event for which alerts must be sent:

- » Select 'When the check fails:' option to send alerts whenever this check fails.
- » Select 'When the check recovers from a failed state' option to send alerts when the monitoring check recovers from a failed state.

4. Select the type of alert to be sent (e.g., click on the 'Send an email to:' option to send email alerts whenever this check fails).



Screenshot 26 - Configuring alert recipients

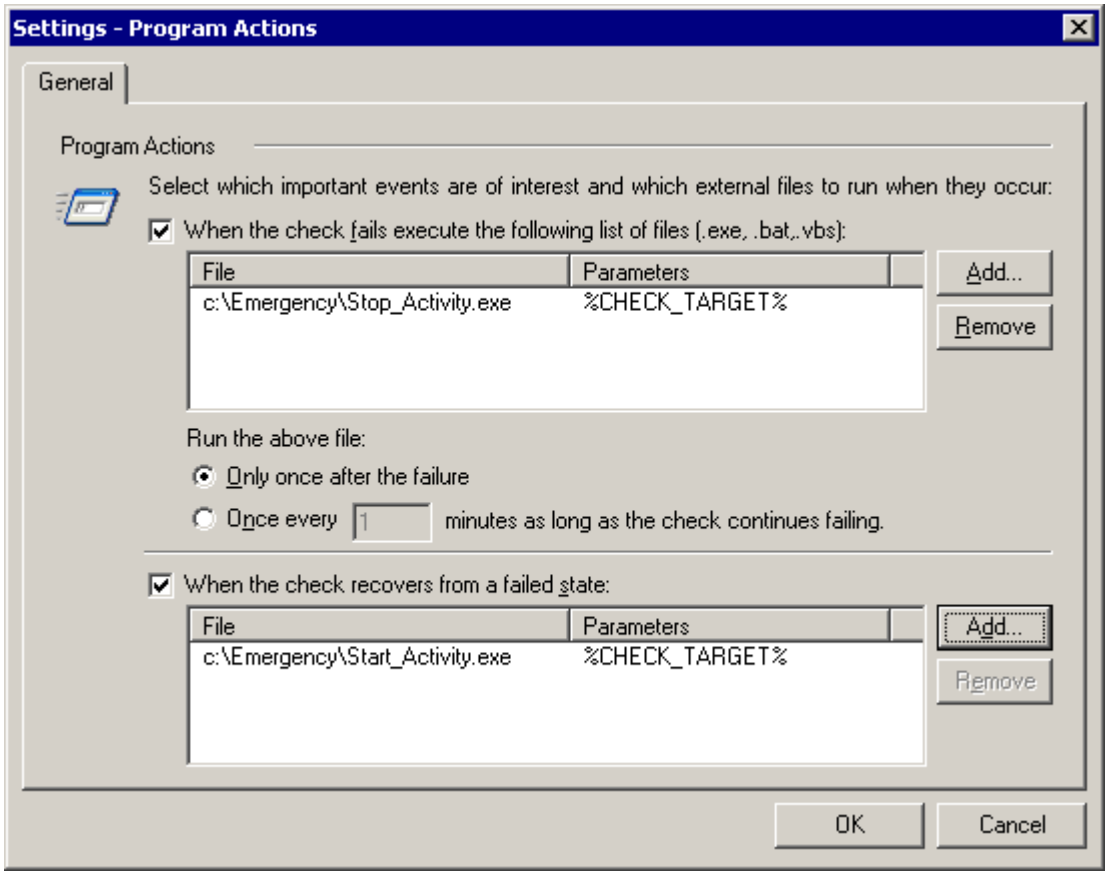
5. Double click on the users and/or groups that must be added to the list of alert recipients. When all the intended recipients have been selected, click on the 'OK' button.

Alerts are sent using the delivery details (email address, etc.) specified in the properties of the selected users. For more information on user properties, please refer to the 'Configure user properties' section in the 'Users and Groups' chapter.

Select the '*Once every …… minutes as long as the check continues failing*' option, ONLY if this alert is to be sent more than once during the time that this check is in a failed state. In this case specify the time interval (in minutes) required between each alert sent. (e.g., To send an alert every 10 minutes, select this option and enter '10' in the time interval to make it read ''*Once every 10 minutes as long as the check continues failing*').

6. Click on 'Apply' to accept the current configuration.

3.4.5 Run an external file after an alert is triggered



Screenshot 27 - Run External File setup dialog

GFI Network Server Monitor can be set up to launch executables, batch and/or VBScript files whenever an important event occurs. This action is configured as follows:

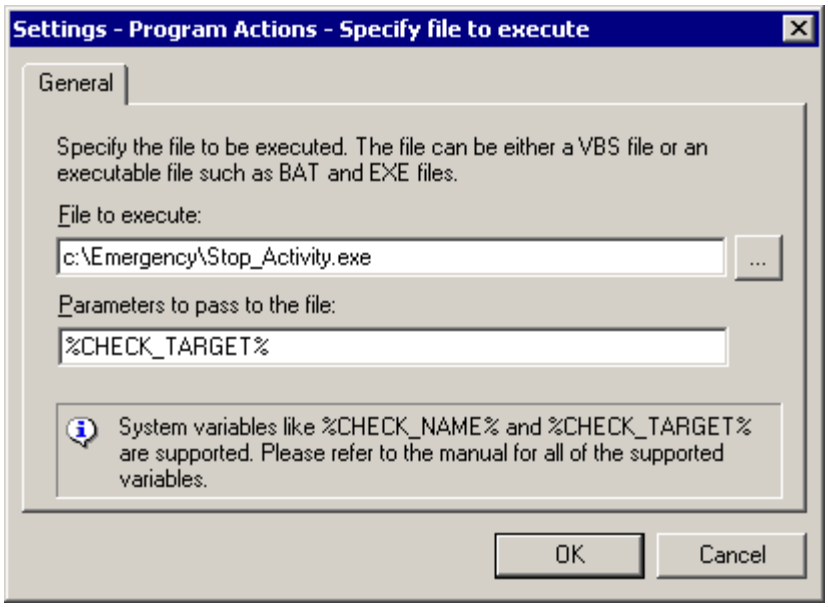
1. Right click on the check to be configured and select 'Properties'. By default the check properties dialog will open in the 'General' tab.

2. Click on the Actions Tab. If the '*Inherit run external file parameters from parent folder*' option is selected, unselect it and click on 'Settings' in the run external file area.

3. Specify the event condition during which the external file will be run:

- » Select 'When the check fails execute…..' option to launch files whenever the check fails.
- » Select 'When the check recovers …' option if you want to launch files when the monitoring check recovers from a failed state.

4. Click on the respective 'Add' button and specify the complete path to the file to be executed (e.g. c:\Error_folder\Capture_Error.exe).


Settings - Program Actions - Specify file to execute
General
Specify the file to be executed. The file can be either a VBS file or an executable file such as BAT and EXE files.
File to execute:
c:\Emergency\Stop_Activity.exe
...
Parameters to pass to the file:
%CHECK_TARGET%
System variables like %CHECK_NAME% and %CHECK_TARGET% are supported. Please refer to the manual for all of the supported variables.
OK
Cancel

Screenshot 28 - File parameters dialog

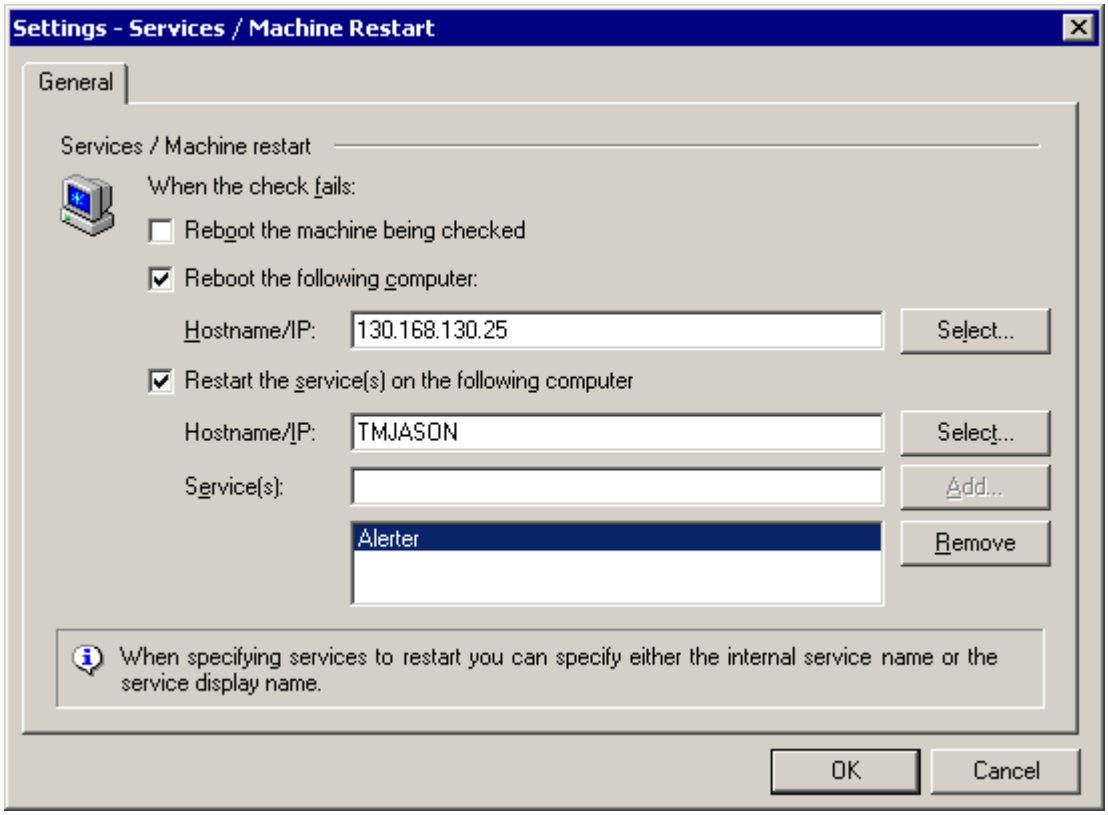
If the file requires any parameters you can still pass them on the command line. You can also pass such parameters through GFI Network Server Monitor, by specifying them in the '*Parameters to pass to the file*' field. You can pass parameters in plain text as well as through variables like <%Date%> and <%CHECK_RESULT%>. These variables are then substituted to values when the program or script is launched. For further information on variables, please refer to the 'Message Templates' section in the 'Global Alerting options' chapter.

5. Click on 'OK' to add this entry to the list of files to be launched.

Select the '*Once every ….. minutes as long as the check continues failing*' option ONLY if this file is to be launched more than once during the time that this check is in a failed state. In this case specify the time interval (in minutes) required between the consecutive execution of the files (e.g., To run a file every 5 minutes, select this option and enter '5' in the time interval so that it reads ''*Once every 5 minutes as long as the check continues failing*').

6. Click on 'Apply' to accept the current configuration.

3.4.6 Restart computers/services after an alert is triggered



Screenshot 29 - Services / Computer restart setup dialog

GFI Network Server Monitor can be set to remotely reboot a computer or restart specific services whenever a monitoring check fails (e.g. if you can't reach an IIS web server in your LAN, you can restart the W3SVC service). Configure this action as follows:

1. Right click on the check to be configured and select 'Properties'. By default the check properties dialog will open in the 'General' tab.

2. Click on the Actions Tab. If the '*Inherit reboot computer/services parameters from Parent folder*' option is selected, unselect it and click on 'Settings' in the run external file area.

3. To reboot the computer being checked, select the '*Reboot the computer being checked*' *option.*

4. To reboot a specific computer:

    (a) Select the '*Reboot the following computer*' option.

    (b) Specify the name or IP address of the computer which will be rebooted (e.g. MAILSERVER).

5. To restart the service(s) on a computer:

    (a) Select the '*Restart the service(s) on the following computer*' option.

    (b) Specify the name or IP address of the target computer on which the service(s) will be restarted.

    (c) Specify the internal or display name (e.g., DNS Client) of the service to be restarted and click on 'Add'. Repeat this step for every service which needs to be restarted.

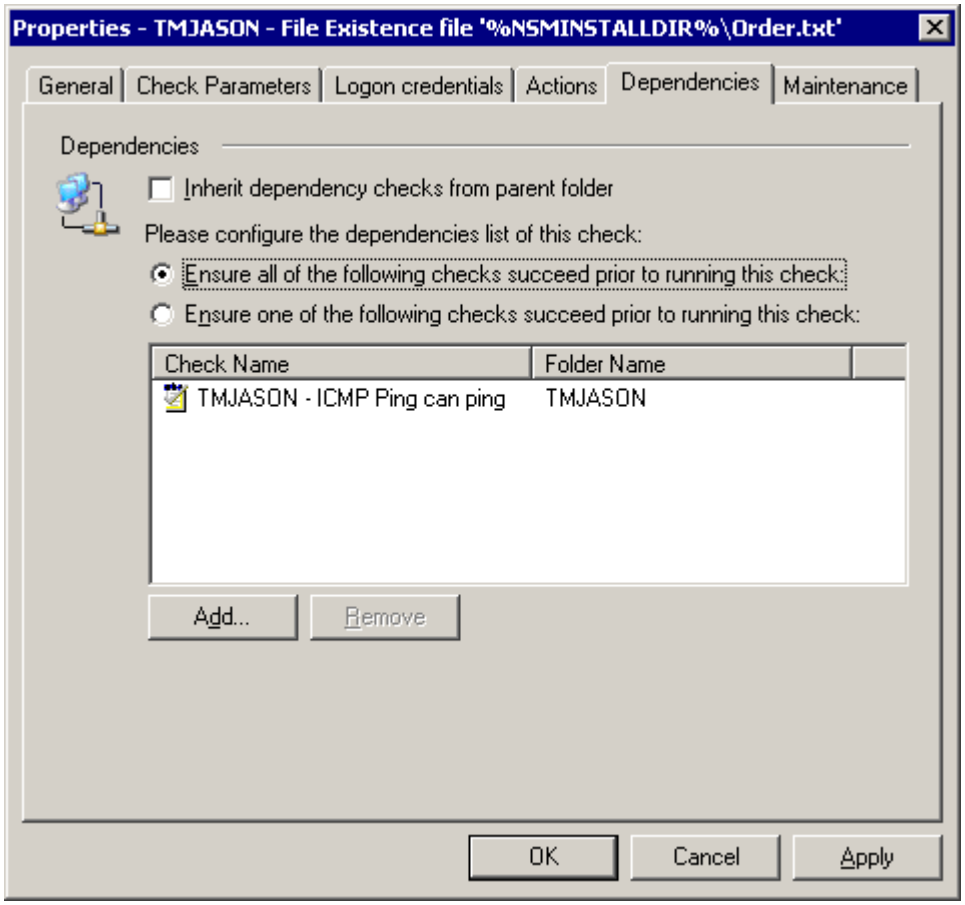
6. Click on 'Apply' to accept the current configuration.

3.4.7 Set up dependencies

Dependencies are checks that define the availability of servers (e.g., ISA Server or Proxy Server) and services (e.g., DNS Server or DNS Client) required by a target computer (i.e., on which a target computer is dependent). The specified dependency check(s) must be successfully executed before the other monitoring checks can be run.

E.g., If you access the Internet through a Proxy Server, an ICMP Ping dependency check can be set to check the availability of the Proxy Server, before executing HTTP/HTTPS monitoring checks. If the dependency check fails, the HTTP/HTTPS check will not be run but will be classified as a 'Failure by Dependee'. For further information on check status classification, please refer to the 'Check State Indicators' section in the 'Monitoring check status' chapter.

TIP: Use dependencies to avoid receiving a flood of alerts, when servers on which other computers depend are down.



Screenshot 30 - Dependencies Setup Dialog

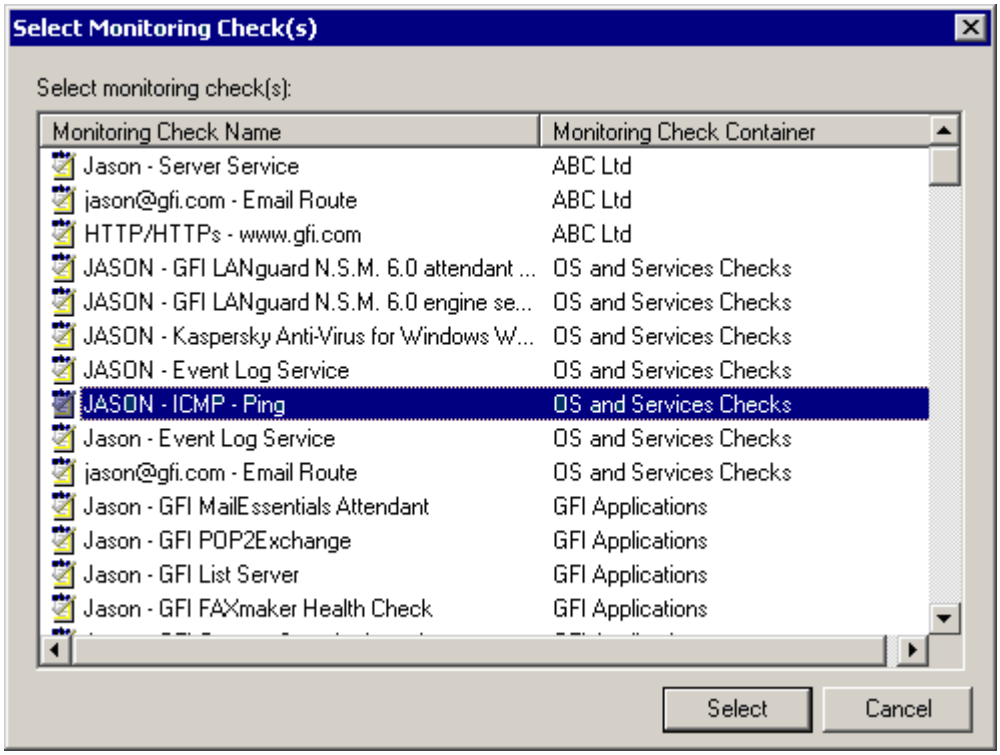
To setup Dependencies:

1. Right click on the check to be configured and select 'Properties'. By default the check properties dialog will open in the 'General' tab.

2. Click on the 'Dependencies' Tab. If the '*Inherit dependency checks from Parent folder*' option is selected, unselect it and choose one of the following dependency conditions:

- » Select the 'Ensure all of the following checks succeed…..' option to denote that ALL checks in the dependency list must be successful before this check is allowed to execute.
- » Select the 'Ensure one of the following checks succeeds…..' option, to denote that at least one of the checks specified in the dependency list must be successful before this check is allowed to execute.

3. Click on 'Add'. Then choose the checks to be included in the dependencies list and click on 'Select'



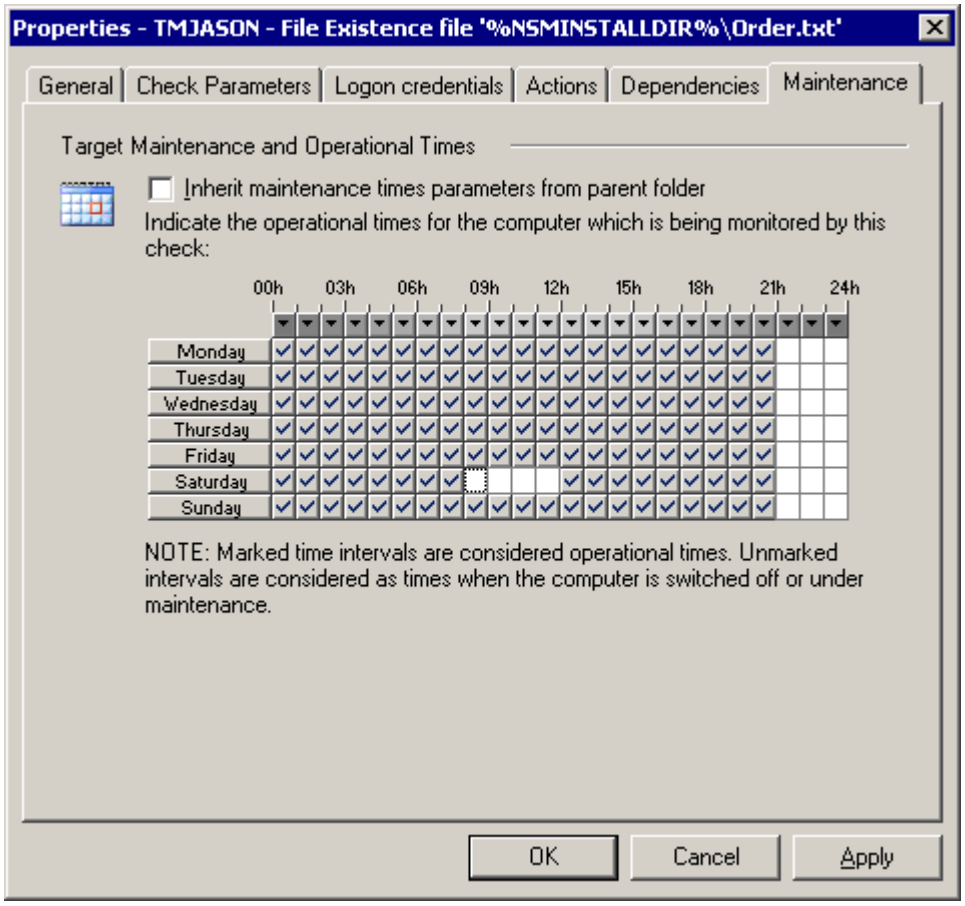
Screenshot 31 - List of available checks

TIP: Multiple check selections are possible by holding down the 'CTRL' or 'SHIFT' keyboard buttons.

4. Click on 'Apply' to accept the current configuration.

3.4.8 Define maintenance schedules

Maintenance parameters define the times during which monitoring check(s) are not executed i.e., during maintenance schedules. These schedules are set up to avoid receiving a flood of alerts when target computers, codependent servers and/or respective services are undergoing maintenance (e.g. during hardware/software upgrades and data backups).



Screenshot 32 - Maintenance schedule Dialog

To set up maintenance schedules:

1. Right click on the check to be configured and select 'Properties'. By default the check properties dialog will open in the 'General' tab.

2. Click on the 'Maintenance' Tab. If the '*Inherit maintenance times parameters from Parent folder*' option is selected, unselect it and specify the operational/maintenance periods for the target computer being monitored.

e.g., The screenshot above shows the maintenance schedule setup for a target computer which is down between 21:00 and 23:00 hrs all week for data backups and between 8:00 and 12:00 hrs every Saturday for hardware and software maintenance.

Marked (✓) time intervals indicate operational times, during which the monitoring check can be run.

3. Click on 'Apply' to accept the current configuration.

TIP 1: To mark/unmark a whole day, click on the name of the day (e.g., Monday) at the left of the hours grid on display.

TIP 2: To mark the same hour for a whole week, click on ▼ at the top of the column representing the required hour.

3.5 Inheriting check properties

About property inheritance

In GFI Network Server Monitor, a parent folder is a folder which contains monitoring checks. Parent folders have properties identical to those configured in monitoring checks. In fact, such folder properties can be configured and then passed on to any/all checks contained in the folder, i.e., they can b inherited.

All properties except for the ‘Check details’ and ‘Check (functional) Parameters’ can be inherited from a parent folder. These include Scan Frequency, Logon credentials, Alerts, and Maintenance parameters among others. For further information on parent folders, please refer to the ‘Check folders’ chapter in this manual.

3.5.1 How to set a folder to inherit properties from a parent folder

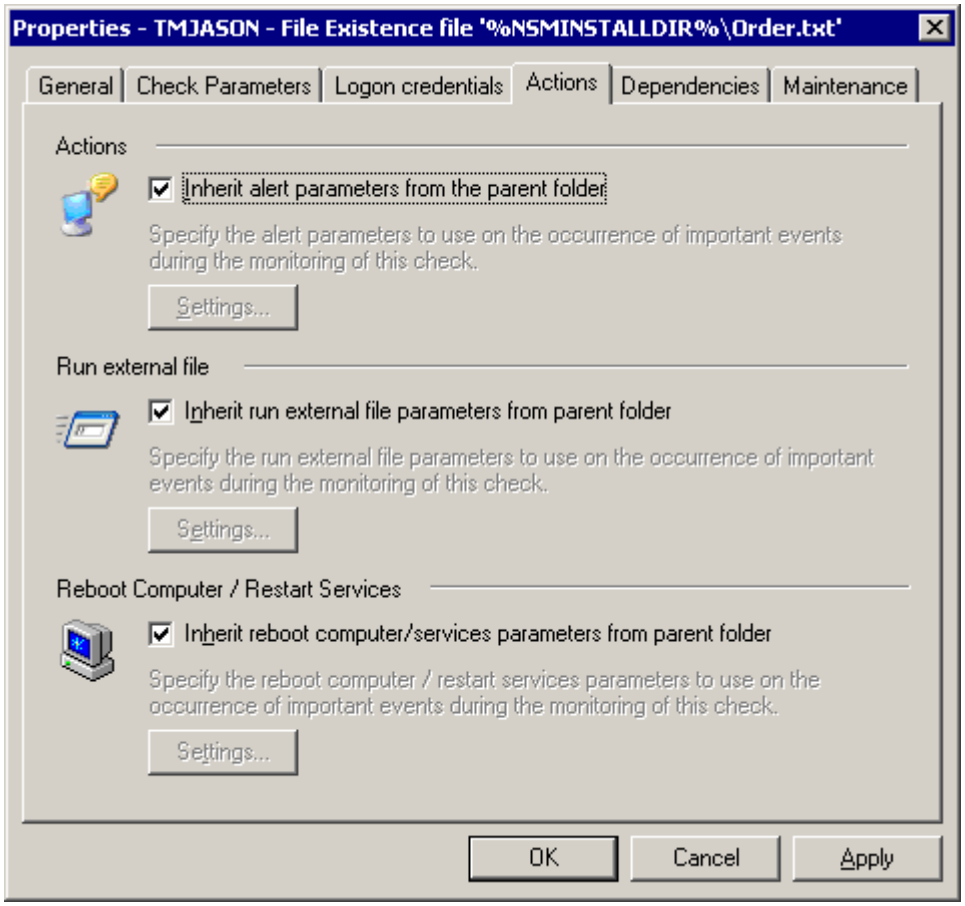
For a folder to inherit properties from a parent folder, select the *‘Inherit ……. from parent folder’* option, present in the check properties that can be inherited.

To inherit the alert settings from a parent folder:

1. Configure the alert parameters on the folder. For more information refer to the ‘Check folders’ chapter in this manual.

2. Select the monitoring check(s) that will inherit the alert parameters. Right click on the selection and choose 'Properties'.

TIP: You can select and set up multiple checks simultaneously by holding down the ‘CTRL’ or ‘SHIFT’ button on the keyboard and selecting the required checks.


Properties - TMJASON - File Existence file '%NSMINSTALLDIR%\Order.txt'
General
Check Parameters
Logon credentials
Actions
Dependencies
Maintenance
Actions
Inherit alert parameters from the parent folder
Specify the alert parameters to use on the occurrence of important events during the monitoring of this check.
Settings...
Run external file
Inherit run external file parameters from parent folder
Specify the run external file parameters to use on the occurrence of important events during the monitoring of this check.
Settings...
Reboot Computer / Restart Services
Inherit reboot computer/services parameters from parent folder
Specify the reboot computer / restart services parameters to use on the occurrence of important events during the monitoring of this check.
Settings...
OK
Cancel
Apply

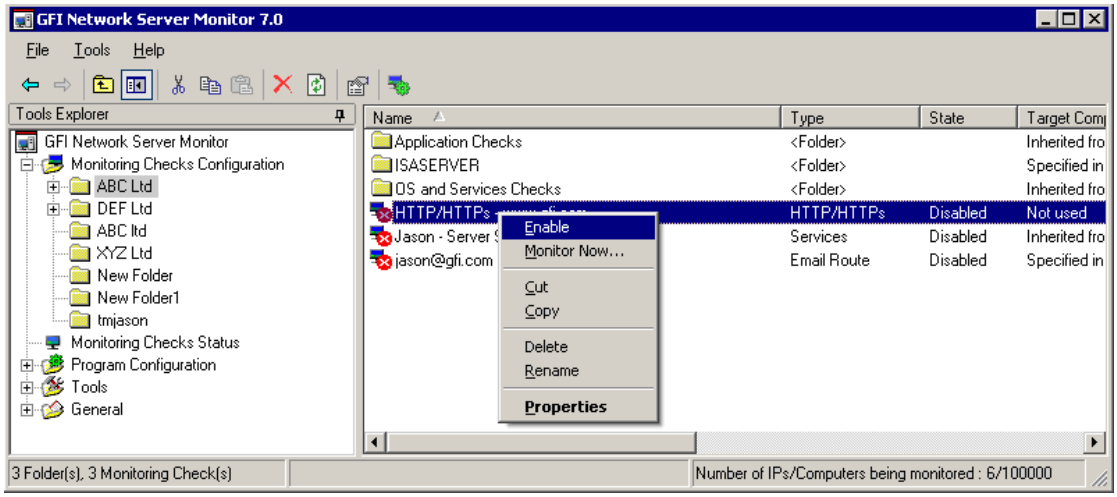
Screenshot 33 - Monitoring check properties - Actions tab setup

3. Click on the ‘Actions’ tab and afterwards, select the *‘Inherit alert parameters from the parent folder’* option.

4. Click on ‘Apply’ to accept this configuration.

It is not possible to set a folder to inherit the parameters of a single alert method (i.e., you cannot inherit just the email alert parameters).

3.6 Enable or disable checks



Screenshot 34 - Check Status display and relative options

GFI Network Server Monitor allows you to enable/disable existing monitoring checks.

The icon on the left of the check details will indicate its state:

- Monitoring check enabled.

- Monitoring check disabled

To enable a monitoring check:

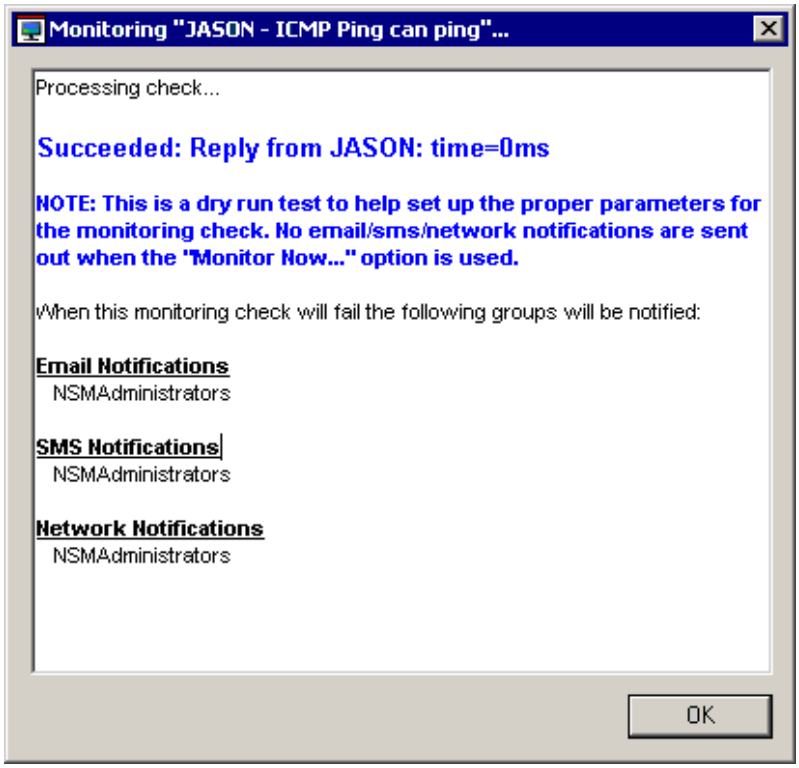
Right click on the monitoring check and select 'Enable'.

To disable a monitoring check:

Right click on the monitoring check and select 'Disable'.

3.7 Testing checks for correctness

To verify that a check is properly configured, right click on a check and select ‘Monitor Now…’.


Monitoring "JASON - ICMP Ping can ping"...
Processing check...
Succeeded: Reply from JASON: time=0ms
NOTE: This is a dry run test to help set up the proper parameters for the monitoring check. No email/sms/network notifications are sent out when the "Monitor Now..." option is used.
When this monitoring check will fail the following groups will be notified:
Email Notifications
NSMAdministrators
SMS Notifications
NSMAdministrators
Network Notifications
NSMAdministrators
OK

Screenshot 35 - The 'Monitor Now' dialog

When running a check through the 'Monitor Now...' utility, no alerts or actions are triggered whenever a check fails.

3.8 Move checks between existing folders

To move checks from one folder to another:

1. Select the check(s), right click on the selection and select ‘Cut’.
2. Right click on the destination folder and select 'Paste'.

3.9 Copy checks from/to existing folders

To copy checks from one folder to another:

1. Select the check(s), right click on the selection and select ‘Copy’.
2. Right click on the destination folder and select 'Paste'.

4 Configuring monitor functions

4.1 Introduction

As soon as the new check wizard is triggered, you must select the required monitor function from the extensive list of built-in functions included in GFI Network Server Monitor. This chapter explains how to configure each built-in function as well as how to create custom monitor functions using VB Scripts. GFI Network Server Monitor groups monitor functions according to their respective role.

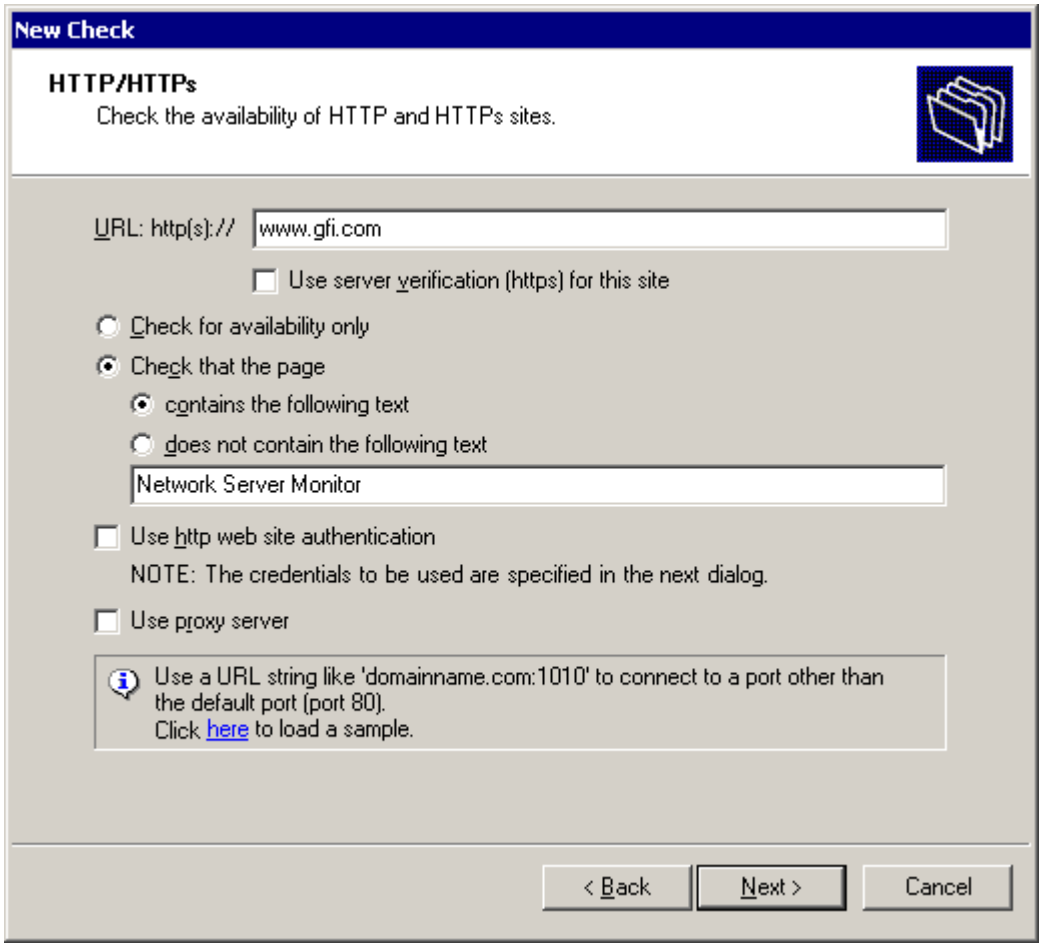
4.2 Network/Internet monitor functions

This group contains functions that are used to monitor Network/Internet protocols and services.

4.2.1 HTTP/HTTPs function

GFI Network Server Monitor can check for the availability of HTTP and HTTPs sites, through specified ports.

GFI Network Server Monitor can be configured to go through a proxy server and to pass access credentials when authentication is required. These credentials can be specified as part of the GFI Network Server Monitor Proxy Server parameters, which are configured from the 'General Options' node. For more information on proxy server parameters, please refer to the 'Proxy Server settings' section in the 'General Options' chapter.


New Check
HTTP/HTTPs
Check the availability of HTTP and HTTPs sites.
URL: http(s)://
www.gfi.com
Use server verification (https) for this site
Check for availability only
Check that the page
contains the following text
does not contain the following text
Network Server Monitor
Use http web site authentication
NOTE: The credentials to be used are specified in the next dialog.
Use proxy server
Use a URL string like 'domainname.com:1010' to connect to a port other than the default port (port 80).
Click here to load a sample.
< Back
Next >
Cancel

Screenshot 36 - HTTP/HTTPS check parameters dialog

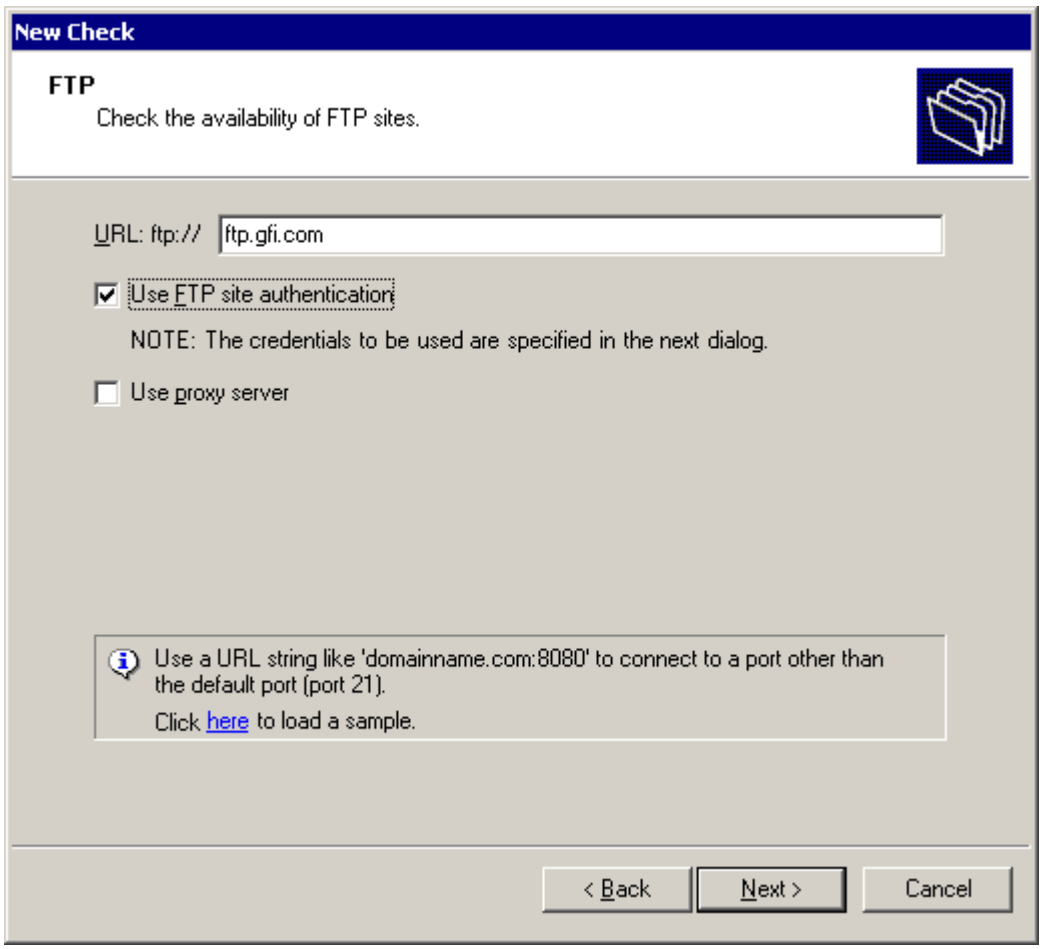
Should the HTTP/HTTPS site require authentication, GFI Network Server Monitor will pass the username and password specified in the Logon Credentials of the monitoring check. For more information on authentication details, please refer to the Logon Credentials section in the 'Configuring GFI Network Server Monitor' chapter.

An HTTP/HTTPs function requires the following parameters:

- URL:http(s):// – Specify the location of the HTTP/HTTPS site in URL format (i.e. http://server[:port]/path/... format).
- Use server verification (https) for this site – Enable, this flag when logon credentials are required to access the target site.
- Check for availability only – Enable this option to check ONLY for the availability of a target site.
- Check availability – Enable this flag to check the availability of a target site as well as to search its contents for a specific string.
- Contains the following text – Enable this flag and specify the string to be searched for, in the contents of the target site. If no match is found, the check will be classified as failed.
- Does not contain the following string – Enable this flag and specify the string to be searched for, in the contents of the target site. If no match is found, then the check is classified as successful.
- Use http web site authentication – Enable this flag if the HTTP target site requires authentication. This option will use the authentication details specified in the logon credentials of the check properties.
- Use proxy server – Enable this flag if the target web site is to be accessed through the Proxy server.

4.2.2 FTP

GFI Network Server Monitor can check the availability of FTP sites through specified ports.


New Check
FTP
Check the availability of FTP sites.
URL: ftp://
ftp.gfi.com
Use FTP site authentication
NOTE: The credentials to be used are specified in the next dialog.
Use proxy server
Use a URL string like 'domainname.com:8080' to connect to a port other than the default port (port 21).
Click here to load a sample.
< Back
Next >
Cancel

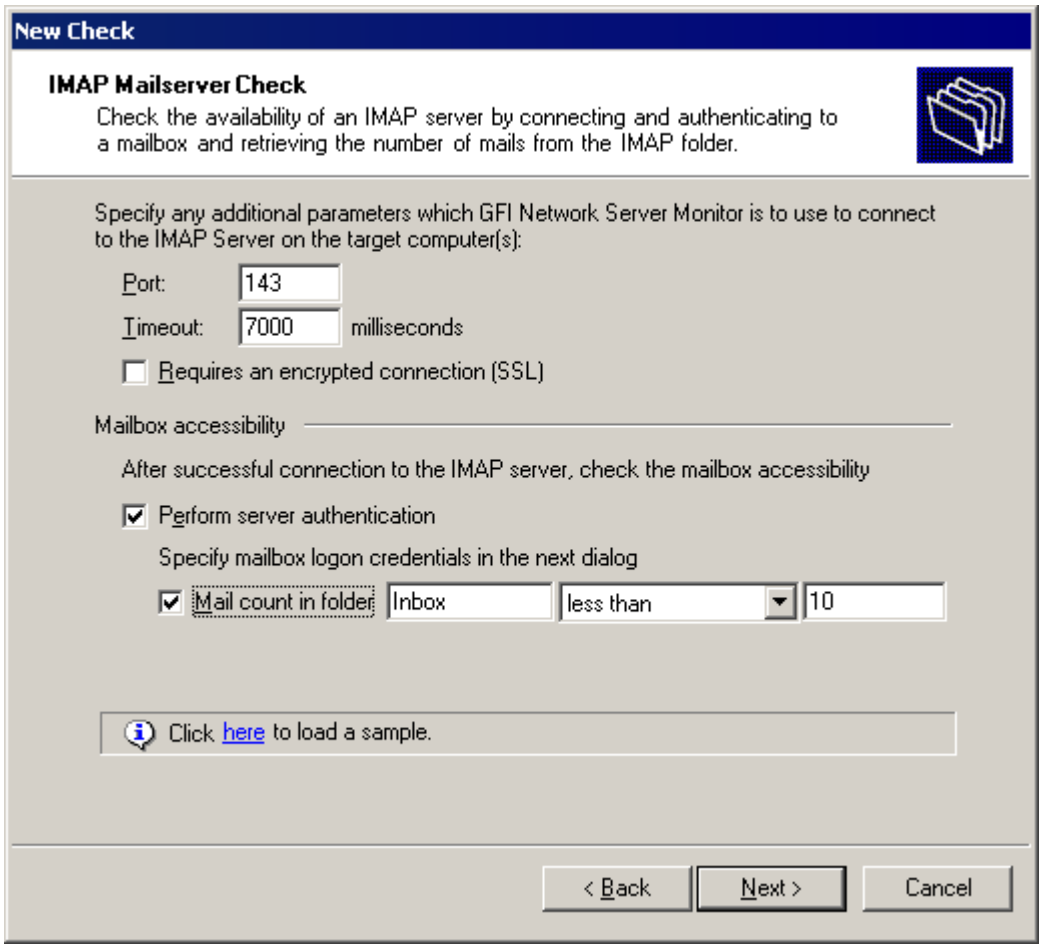
Screenshot 37 - FTP check parameters dialog

GFI Network Server Monitor can be configured to go through a proxy server as well as to pass access credentials to the specified FTP site should authentication be required.

- An FTP monitor function requires the following parameters:
- URL:ftp(s):// – Specify the location of the ftp site in URL format (i.e. ftp://server[:port]/path/... format).
- Use FTP site authentication – Enable this flag when logon credentials are required to access the specified FTP site.
- Use Proxy server – Enable this flag if the specified FTP site is to be accessed through a Proxy server.

4.2.3 IMAP Mailserver check

GFI Network Server Monitor can check the availability of IMAP mail servers. The IMAP Mailserver check initiates a handshake connection to the remote IMAP port and through the replies received, it can verify if the remote server's IMAP protocol is working properly. This check can also be configured to physically log on to a specific mailbox and check for the number of emails present in a folder within the accessed mailbox. This will verify that the IMAP service is indeed running, accessible and delivering the service required to the end users. The IMAP check also supports logon to the IMAP mailbox using SSL. Through SSL, you can secure the transmission session by electronically authenticating each end of an encrypted transmission.


New Check
IMAP Mailserver Check
Check the availability of an IMAP server by connecting and authenticating to a mailbox and retrieving the number of mails from the IMAP folder.
Specify any additional parameters which GFI Network Server Monitor is to use to connect to the IMAP Server on the target computer(s):
Port:
143
Timeout:
7000
milliseconds
Requires an encrypted connection (SSL)
Mailbox accessibility
After successful connection to the IMAP server, check the mailbox accessibility
Perform server authentication
Specify mailbox logon credentials in the next dialog
Mail count in folder
Inbox
less than
10
Click here to load a sample.
< Back
Next >
Cancel

Screenshot 38- IMAP server check parameters dialog

The IMAP check requires the following parameters:

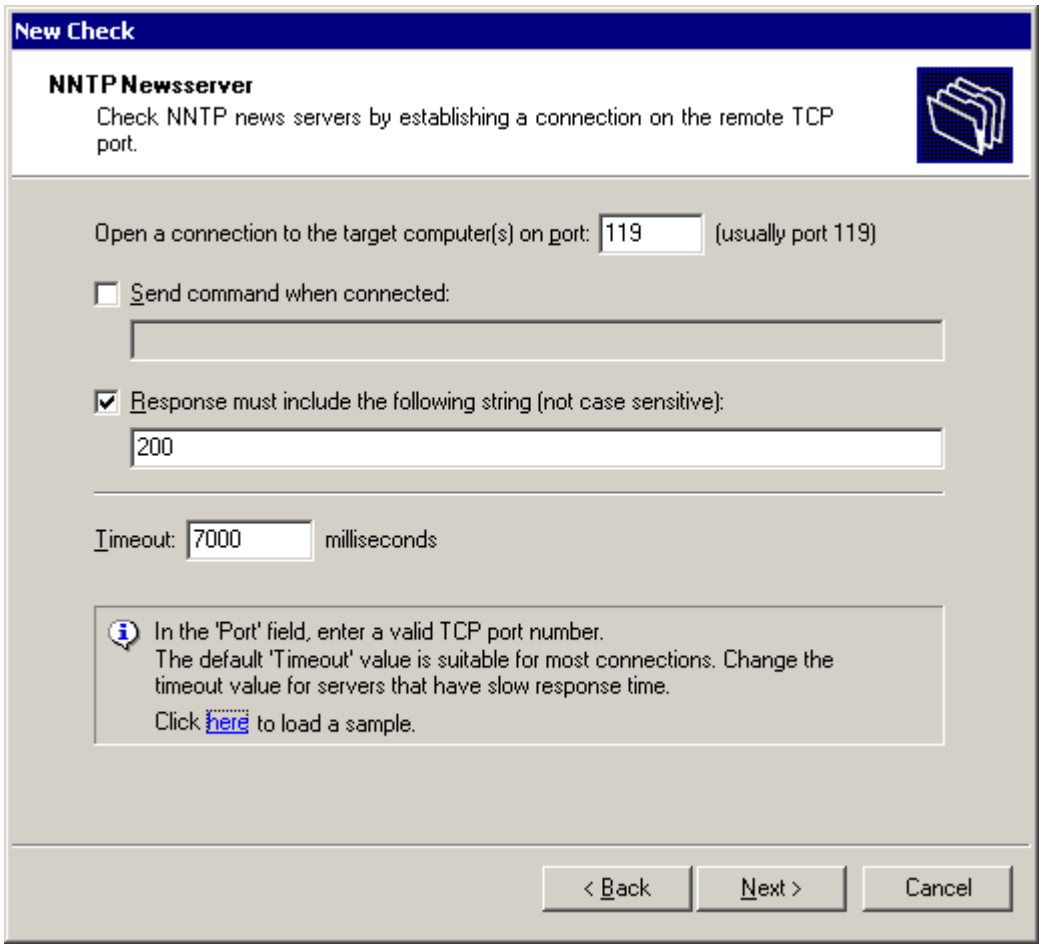
- Port – Specify the TCP port to be used when connecting to the IMAP mail server (IMAP default port is 143).
- Timeout – Specify the connection timeout in milliseconds. The check will fail if a connection is not established before the specified timeout passes.

- Requires an encrypted connection (SSL) – Select this option if you want to encrypt the data during transmission.
- Login to mailbox – Select this option if you want to physically check whether a mailbox on your mail server can be logged on to.
- Mail count in folder - Select this option if you want the check to fail/succeed based on the number of emails present in a folder on the IMAP server. In addition, you must specify the:
  - IMAP folder name (e.g. Inbox)
  - Logical comparison operator: Specify if the count should be 'equal to', 'not equal to', 'less than', 'less than or equal to', 'greater than', 'greater than or equal to' a specified value.
  - The value (i.e., the number of emails) to which the retrieved count will be compared.

When the 'Login to mailbox' option is selected, alternative credentials will be required so that this check can remotely log on to the mailbox on your IMAP server. The New Check Wizard automatically prompts you to configure these alternative credentials (i.e., the user name and password) during the creation of this check. After the check has been created, you can make changes to alternative credentials from the Check properties dialog > 'Logon Credentials' tab.

4.2.4 NNTP news server availability

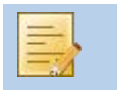
GFI Network Server Monitor can check NNTP news servers by starting a handshake connection on the remote TCP port (normally port 119). By handshaking, GFI Network Server Monitor can verify that the remote server's NNTP protocol is online and functional.


New Check
NNTP Newsserver
Check NNTP news servers by establishing a connection on the remote TCP port.
Open a connection to the target computer(s) on port: 119 (usually port 119)
Send command when connected:
Response must include the following string (not case sensitive):
200
Timeout: 7000 milliseconds
In the 'Port' field, enter a valid TCP port number.
The default 'Timeout' value is suitable for most connections. Change the timeout value for servers that have slow response time.
Click here to load a sample.
< Back
Next >
Cancel

Screenshot 39 - NNTP Server check parameters dialog

An NNTP news server availability function requires the following parameters:

- Port – Specify the TCP port number to be used when connecting to NNTP news server. (NNTP Default port is 119).
- Send command when connected – Enable this flag to send a specified command as soon as the connection is established.
- Response must include the following string – Enable this flag in order to check if the response message contains a specified string.

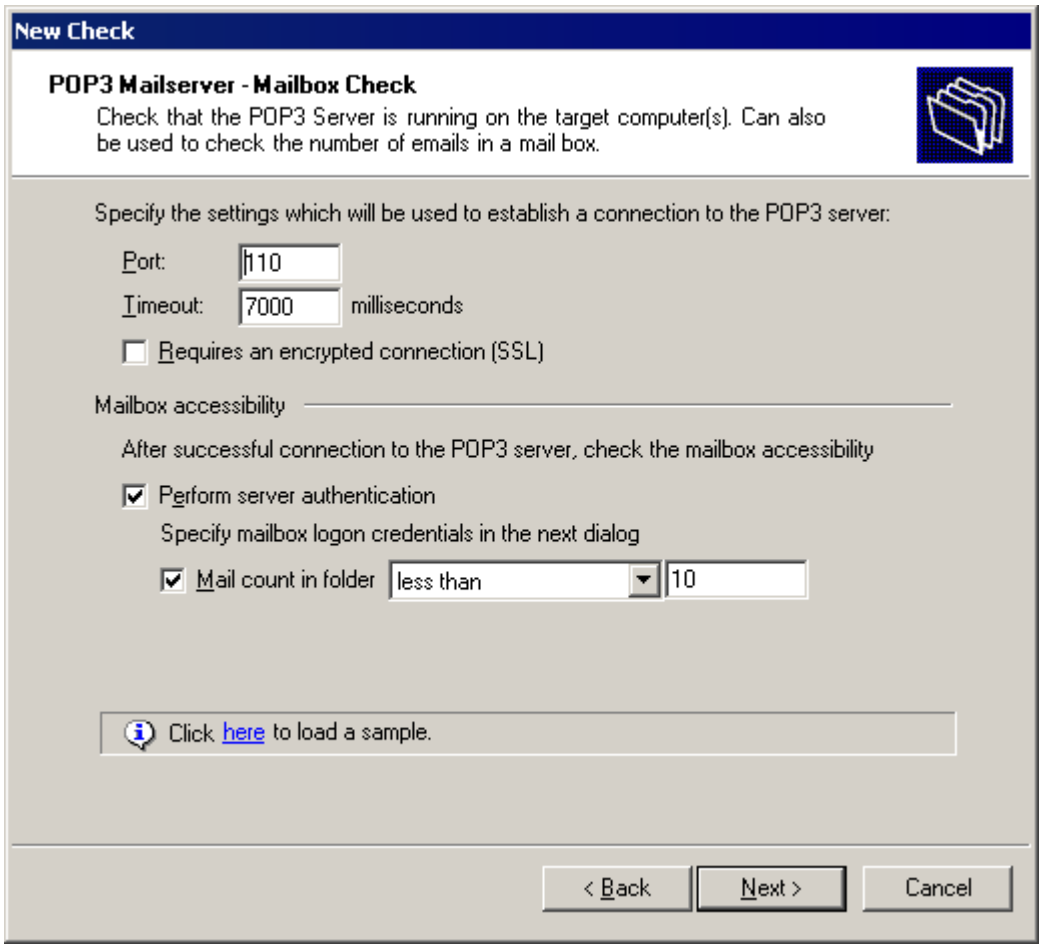


Normally a response from NNTP servers includes: '200' in its string.

- Timeout – Specify the number of milliseconds before the function will timeout. Usually, a connection to the server will be established within 1 second. However, some slow/busy servers need more time. Default value is set to 7000 milliseconds.

4.2.5 POP3 Mailserver check

GFI Network Server Monitor can check the availability of POP3 mail servers. The POP3 Mailserver check initiates a handshake connection to the remote POP3 port and through the replies received, it can verify if the remote server's POP3 protocol is working properly. This check can also be configured to physically log on to a specific mailbox and check for the number of emails present in a folder within the accessed mailbox. This will verify that the POP3 service is indeed running, accessible and delivering the required service to end users. The POP3 check also supports logon to the POP3 mailbox using SSL. Through SSL, you can secure the transmission session by electronically authenticating each end of an encrypted transmission.


New Check
POP3 Mailserver - Mailbox Check
Check that the POP3 Server is running on the target computer(s). Can also be used to check the number of emails in a mail box.
Specify the settings which will be used to establish a connection to the POP3 server:
Port:
110
Timeout:
7000
milliseconds
Requires an encrypted connection (SSL)
Mailbox accessibility
After successful connection to the POP3 server, check the mailbox accessibility
Perform server authentication
Specify mailbox logon credentials in the next dialog
Mail count in folder
less than
10
Click here to load a sample.
< Back
Next >
Cancel

Screenshot 40 - POP3 server check parameters dialog

The POP3 Mailserver check requires the following parameters:

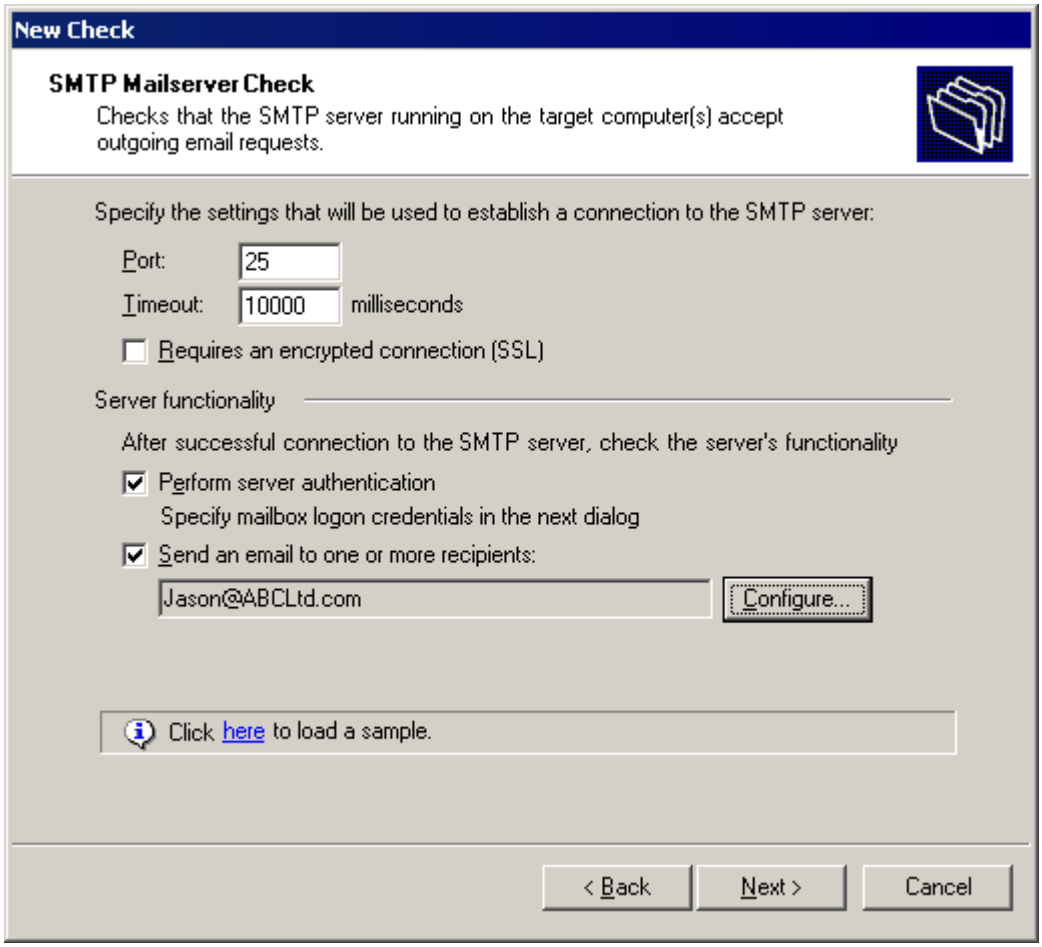
- Port – Specify the TCP port to be used when connecting to the POP3 mail server (POP3 Default port is 110).
- Timeout – Specify the connection timeout in milliseconds. The check will fail if a connection is not established before the specified timeout elapses.
- Requires an encrypted connection (SSL) – Select this option if you want to encrypted the transmission (i.e. establish a secure session by electronically authenticating each end of an encrypted transmission).
- Login to mailbox – Select this option if you want to verify mail box authentication on your mail server.
- Mail count in folder - Select this option if you want to count the number of emails in a POP3 mail box. In addition, you must specify the:
  - Logical comparison operator: State if the count should be 'equal to', 'not equal to', 'less than', 'less than or equal to', 'greater than', 'greater than or equal to' a specified value.
  - The value (i.e., the number of emails) to which the retrieved count will be compared to.

When the 'Login to mailbox' option is selected, alternative credentials will be required so that this check can remotely log on to the mailbox on your POP3 server. The New Check Wizard automatically prompts you to configure these alternative credentials (i.e., the user name and password) during the creation of this check. After the check has been created, you can make changes to alternative credentials from the Check properties dialog > 'Logon Credentials' tab.

4.2.6 SMTP Mailserver check

GFI Network Server Monitor can check the availability of SMTP mail servers. The SMTP Mailserver check initiates a handshake connection to the remote SMTP port and through the replies received, it can verify if the remote server's SMTP protocol is working properly. This check can also be configured to physically log on to the server (where applicable) and gain access to the SMTP service. Once logon is authorized, the SMTP check can also send a physical test email to a target email address. This will verify that the SMTP service is indeed running, accessible and delivering the required service to end users.

The SMTP check also supports logon to the SMTP server using SSL. Through SSL, you can secure the transmission session by electronically authenticating each end of an encrypted transmission.


New Check
SMTP Mailserver Check
Checks that the SMTP server running on the target computer(s) accept outgoing email requests.
Specify the settings that will be used to establish a connection to the SMTP server:
Port: 25
Timeout: 10000 milliseconds
Requires an encrypted connection (SSL)
Server functionality
After successful connection to the SMTP server, check the server's functionality
Perform server authentication
Specify mailbox logon credentials in the next dialog
Send an email to one or more recipients:
Jason@ABCLtd.com
Configure...
Click here to load a sample.
< Back
Next >
Cancel

Screenshot 41 - SMTP server check parameters dialog

The SMTP Mailserver check requires the following parameters:

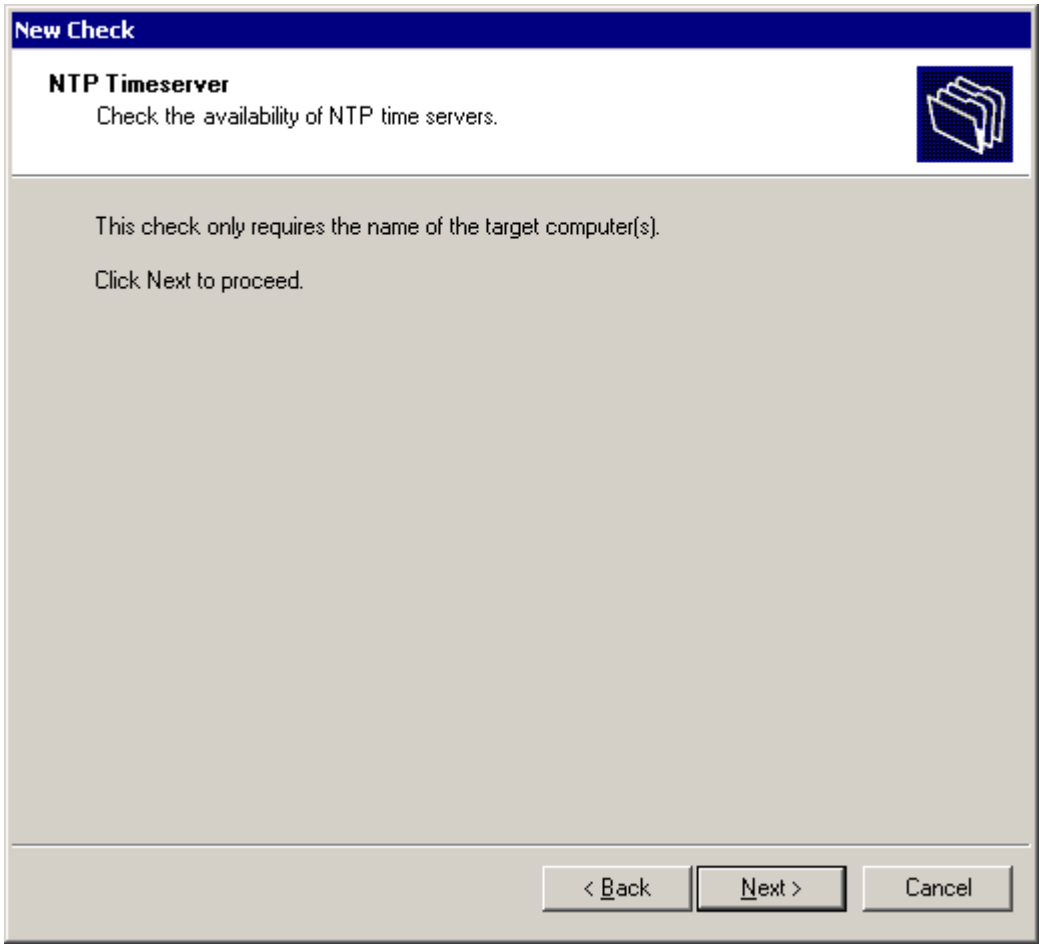
- Port – Specify the TCP port to be used when connecting to the SMTP mail server (SMTP Default port is 25).
- Timeout – Specify the connection timeout in milliseconds. The check will fail if a connection is not established before the specified timeout elapses.
- Requires an encrypted connection (SSL) – Select this option if you want to encrypted the transmission (i.e. establish a secure session by electronically authenticating each end of an encrypted transmission).
- Login to mailbox – Select this option if you want to verify mail box authentication on your mail server.
- Send an email to one or more recipients – Select this option if you want to verify your SMTP server's functionality by sending a test email to particular recipients. To specify the sender and recipient(s) email address, click on 'Configure'.

When the 'Login to mailbox' option is selected, alternative credentials will be required so that this check can remotely logon to the mailbox on your SMTP server. The New Check Wizard automatically prompts you to configure these alternative credentials (i.e., the user name and password) during the creation of this check. After the check has been created, you can make changes to alternative credentials from the Check properties dialog > 'Logon Credentials' tab.

4.2.7 NTP Time Server availability

Most of organizations use a time server to ensure accurate time settings. The NTP protocol is the protocol used to synchronize times between workstations/servers, and external time sources.

GFI Network Server Monitor uses NTP to check the availability of internal and external time sources.


New Check
NTP Timeserver
Check the availability of NTP time servers.
This check only requires the name of the target computer(s).
Click Next to proceed.
< Back
Next >
Cancel

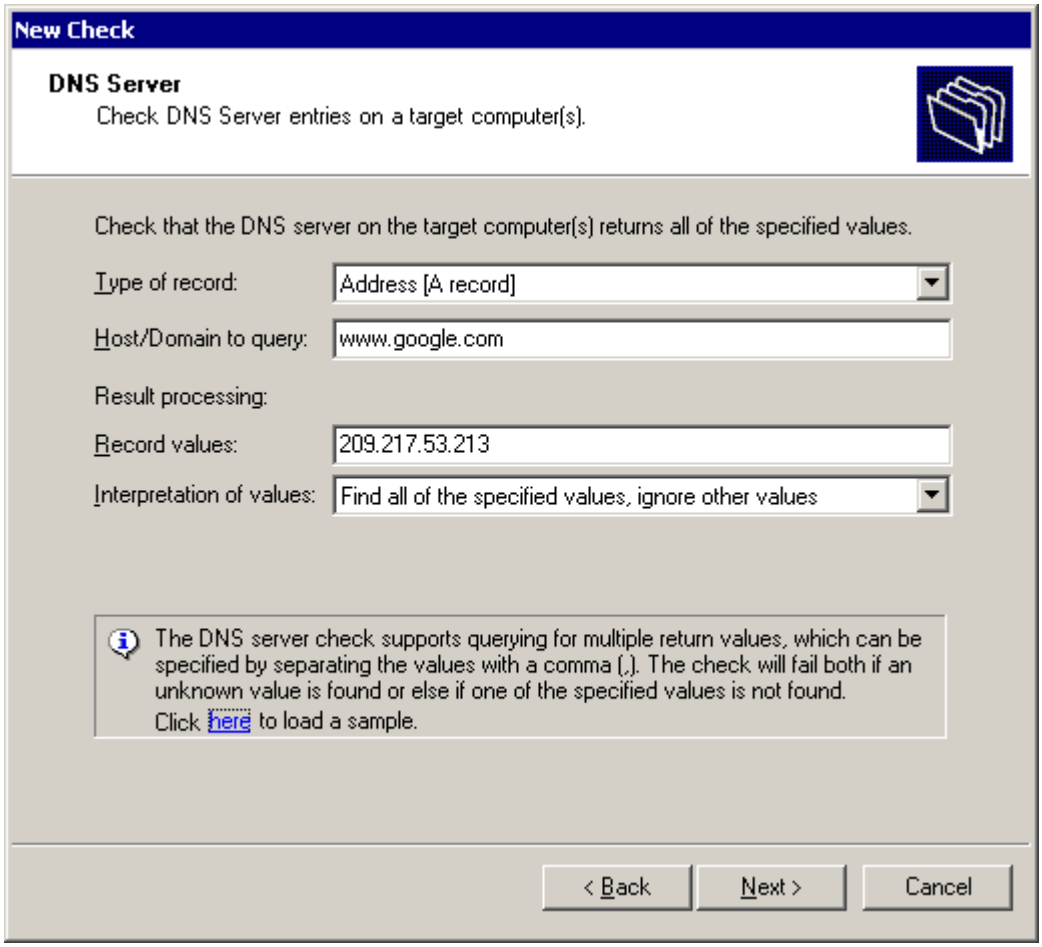
Screenshot 42- NTP Time server check parameters dialog

The NTP function requires NO parameters.

4.2.8 DNS server check

The DNS server check can read a specific 'record' type on a DNS server and then compare it to a specified (expected result) value. In addition, you can also specify how this check will interpret the result after comparing the value returned by the DNS server to the parameter specified in the 'Record values' field.

For example, this check can read the 'A record' (address record) from the DNS server and verify if it includes the IP address specified in the expected result field (i.e., 'Record values' field).


New Check
DNS Server
Check DNS Server entries on a target computer(s).
Check that the DNS server on the target computer(s) returns all of the specified values.
Type of record:
Address [A record]
Host/Domain to query:
www.google.com
Result processing:
Record values:
209.217.53.213
Interpretation of values:
Find all of the specified values, ignore other values
The DNS server check supports querying for multiple return values, which can be specified by separating the values with a comma (,). The check will fail both if an unknown value is found or else if one of the specified values is not found.
Click here to load a sample.
< Back
Next >
Cancel

Screenshot 43 - DNS server check parameters dialog

The DNS server check requires the following parameters:

- Type of record – Specify the record type which needs to be defined by the DNS server. This can be an A record or any other record type present in the drop down list.
- Host/Domain Name to query – Specify the hostname or domain that you wish to resolve (E.g., www.google.com).
- Record values – Specify the expected return value(s). This is the value/string which will be compared to the value returned by the DNS Server (i.e., the return value).
- E.g., If an A record type was selected, the check will query the DNS server to resolve the IP address of the host/domain specified in the 'Host/Domain to query' field. This query should return one or more IP addresses which will be compared to the IP(s) specified in the 'Record Values' field.

Since a DNS query can return more than one IP address, this check allows you to specify multiple return values separated by a comma (,) e.g., 209.217.53.213,66.172.16.32.

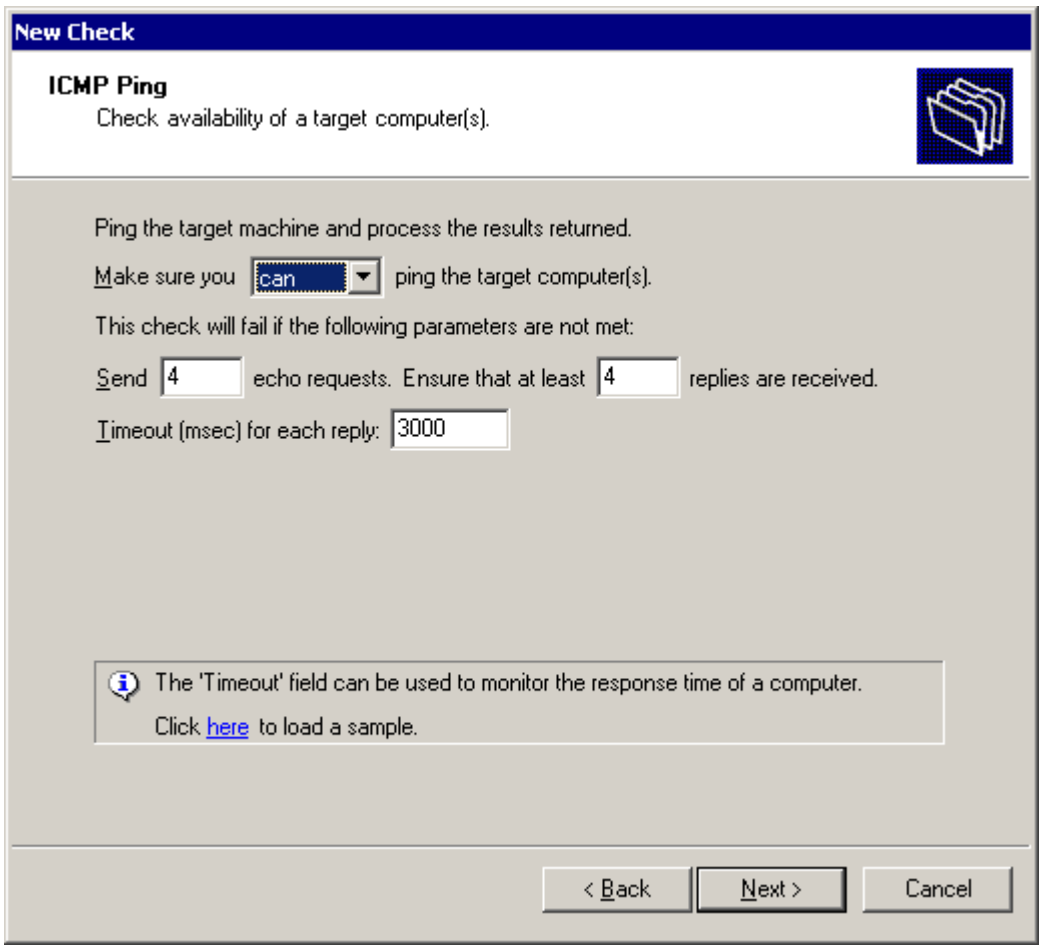
- Interpretation of values – Specify how this check will interpret the result after comparing the returned value to the parameter specified in the 'Record values' field.

  E.g., If you select "Find all of the specified values, fail if other values are found", the check will fail only if the returned value does not entirely match to the value specified in the 'Record values' field.

4.2.9 ICMP/Ping

The ICMP Ping function checks the availability of a remote host by sending ICMP Echo commands and waiting for the response from the host.

Although local hosts should normally respond to ping requests within milliseconds, an ICMP timeout failure doesn't necessarily mean that the remote host is actually functioning beyond its ability to echo packets.


New Check
ICMP Ping
Check availability of a target computer(s).
Ping the target machine and process the results returned.
Make sure you can ping the target computer(s).
This check will fail if the following parameters are not met:
Send 4 echo requests. Ensure that at least 4 replies are received.
Timeout (msec) for each reply: 3000
The 'Timeout' field can be used to monitor the response time of a computer.
Click here to load a sample.
< Back
Next >
Cancel

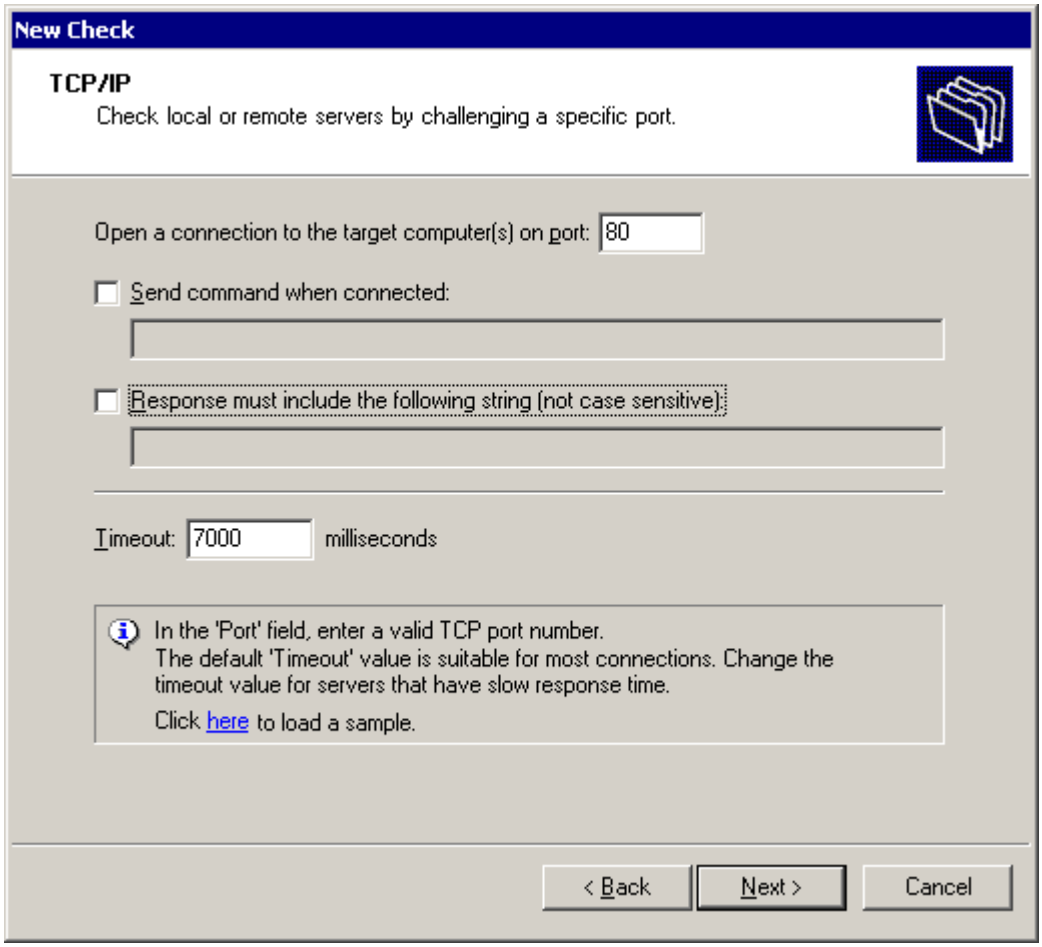
Screenshot 44 - ICMP/Ping check parameters dialog

The ICMP/Ping function requires the following parameters:

- *Make sure you…..ping the target computer* – Select 'Can' to specify that the check is successful if the server replies to the ping. Select 'Cannot' to specify that the check fails if the server replies to the ping.
- Number of Echo requests to send – Specify the number of pings to be sent.
- Minimum number of expected replies – Specify the minimum number of replies that must be received for the check to be successful.
- Timeout (m.sec) for each reply – Specify the expected response time (in milliseconds). This is the time that the check will wait for a response to an echo request (i.e. the time between successive echo requests).

4.2.10 Generic TCP/IP check

GFI Network Server Monitor can check local or remote server connections by challenging a specific port. The challenge will involve connecting to the target computer, sending it a sequence of bytes and analyzing the information received.


New Check
TCP/IP
Check local or remote servers by challenging a specific port.
Open a connection to the target computer(s) on port: 80
Send command when connected:
Response must include the following string (not case sensitive):
Timeout: 7000 milliseconds
In the 'Port' field, enter a valid TCP port number.
The default 'Timeout' value is suitable for most connections. Change the timeout value for servers that have slow response time.
Click here to load a sample.
< Back
Next >
Cancel

Screenshot 45 - TCP/IP check parameters dialog

A TCP/IP check requires the following parameters:

- Port – Specify the TCP port number of the protocol to be checked, by default port 80.
- Send command when connected – Enable this flag to send the specified command as soon as the connection is established.
- Response must include the following string – Enable this flag in order to check if the response message contains the specified string.
- Timeout – Number of milliseconds before the function will timeout. Usually, a connection to the server will be established within 1 second. However, some slow/busy servers need more time. Recommended value is 7000 milliseconds.

4.2.11 Email Route check

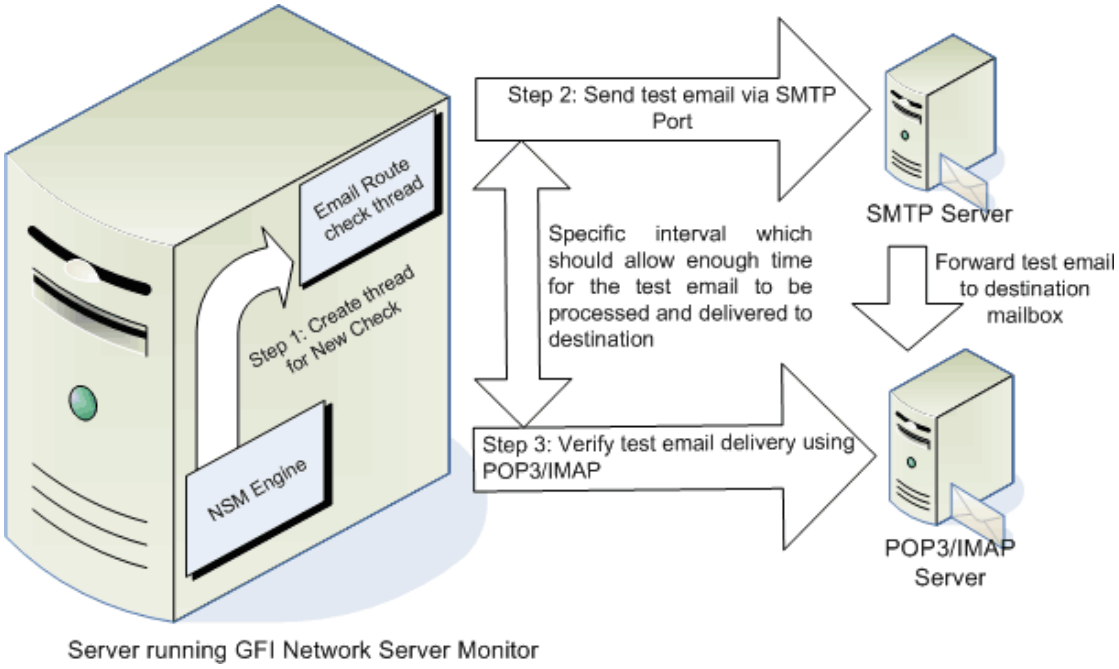
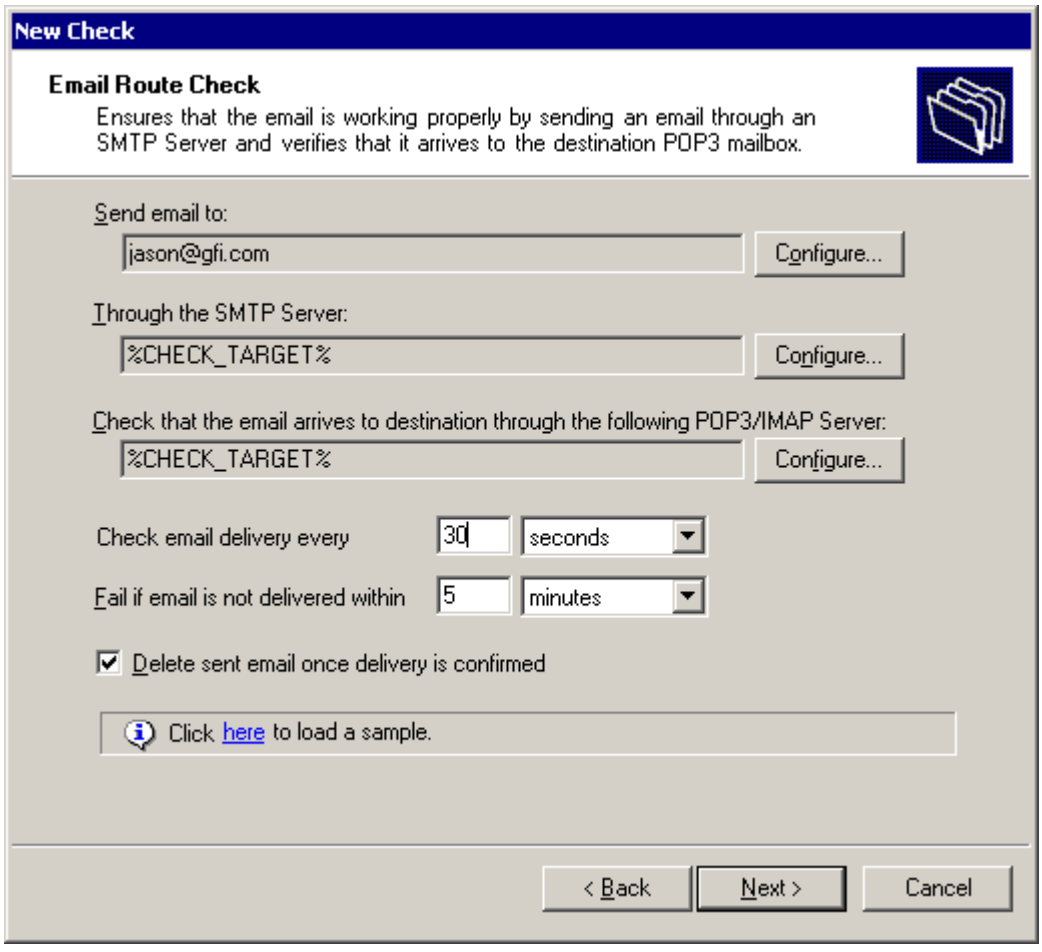

Email Route check thread
Step 1: Create thread for New Check
NSM Engine
Server running GFI Network Server Monitor
Step 2: Send test email via SMTP Port
SMTP Server
Specific interval which should allow enough time for the test email to be processed and delivered to destination
Forward test email to destination mailbox
Step 3: Verify test email delivery using POP3/IMAP
POP3/IMAP Server

Figure 1 - Email Route check operation

The Email Route check verifies if your email services are working properly; it does so by sending a physical email through a target SMTP server and checking for the arrival of the test email in a mailbox on a target POP3 Server.


New Check
Email Route Check
Ensures that the email is working properly by sending an email through an SMTP Server and verifies that it arrives to the destination POP3 mailbox.
Send email to:
jason@gfi.com
Configure...
Through the SMTP Server:
%CHECK_TARGET%
Configure...
Check that the email arrives to destination through the following POP3/IMAP Server:
%CHECK_TARGET%
Configure...
Check email delivery every
30
seconds
Fail if email is not delivered within
5
minutes
Delete sent email once delivery is confirmed
Click here to load a sample.
< Back
Next >
Cancel

Screenshot 46 - Email Route check dialog

To configure the Email Route check, you must specify:

- The sender's and recipient's email address. For more information on how to configure these parameters refer to the 'Configuring the sender's and recipient's email address' section.
- The SMTP server through which the test email will be sent (i.e., the SMTP server to be checked). For more information on how to configure these parameters, refer to the 'Configuring the SMTP Server details' section below.
- The POP3/IMAP server through which the test email will be delivered (i.e., the POP3/IMAP server to be checked). For more information on how to configure these parameters, refer to the 'Configuring the POP3/IMAP Server details' section below.
- The frequency at which this check will verify if the test email was delivered to the destination mailbox. This means that if you set the check email delivery value to 30 seconds, this check will access the destination mailbox two times per minute until the email is found or until the (test) email delivery is timed out.

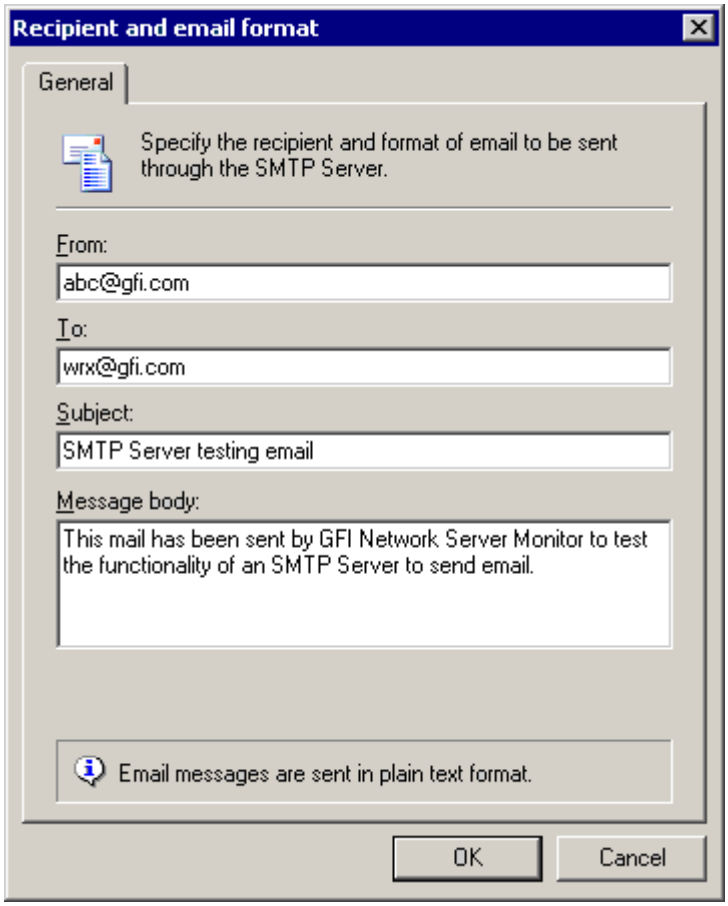
You cannot configure a 'Check email delivery …' value which is greater than the specified timeout value.

- The test-email delivery timeout value. This is the time during which the check will verify if the test email was delivered to the destination mailbox. In other words, this is the time allocated for the test email to travel between the SMTP server and the destination mailbox. If the email is not delivered to destination within the specified time, a timeout occurs and the Email route check will fail.
- Optionally, GFI Network Server Monitor can delete the test email once the delivery is confirmed. To automatically delete the test email, select the 'Delete sent email once delivery is confirmed' option at the bottom of the Email Route check parameters dialog.

The Email Route check is successful ONLY if the test email is present in the destination mailbox. This means that on heavy-traffic or slow networks, you must configure enough delay between the sending and the verification of delivery stages to allow enough time for the test email to arrive to destination.

Make sure that the email client of the recipient (i.e., the person to whom you have addressed the test email) is not open. Otherwise, the test email might be immediately downloaded from the POP3/IMAP server to the client before the delivery verification takes place, hence causing the check to fail. A separate mailbox which is used only by GFI Network Server Monitor should be used.

Configuring the sender's and recipient's email address


Recipient and email format
General
Specify the recipient and format of email to be sent through the SMTP Server.
From:
abc@gfi.com
To:
wrx@gfi.com
Subject:
SMTP Server testing email
Message body:
This mail has been sent by GFI Network Server Monitor to test the functionality of an SMTP Server to send email.
Email messages are sent in plain text format.
OK
Cancel

Screenshot 47 - The test email details dialog

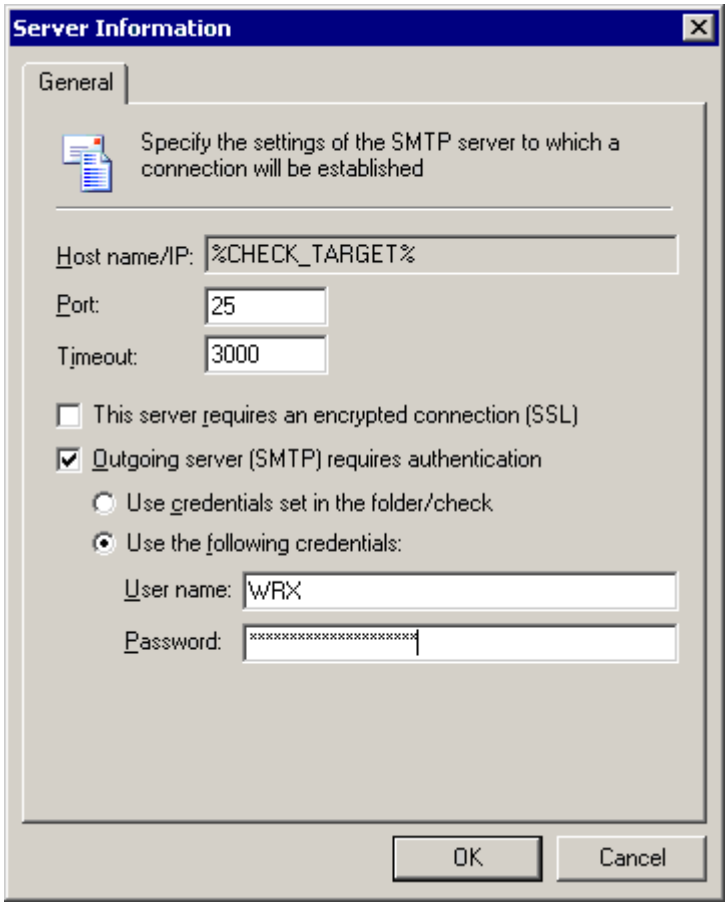
Click on the 'Configure' button of the relevant section to specify the following parameters:

- From – Specify the sender's email address (i.e., the email account from where the test email will be sent).
- To – Specify the recipient's email address (i.e., the email account where the test email will be sent).
- Subject – (Optional) Specify the text to be included in the subject field of the test email.
- Message - (Optional) Specify the text to be included in the message body.

Test email messages can only be sent in plain text format.

When all required details have been specified, click on 'OK' to save and return to the Email Route check properties dialog.

4.2.12 Configuring the SMTP Server details



Screenshot 48 - SMTP Server configuration dialog

Click on the 'Configure' button of the relevant section to specify the following parameters:

The 'Host name/IP' parameter contains the details of the SMTP Server to which the connection will be established. This parameter cannot be changed and it is configured to acquire its value from the %CHECK_TARGET% variable. This variable takes its value directly from the Target Computer field in the Check properties. This means that you must specify the correct Target Computer details (i.e., the hostname/IP of your SMTP server) in the Check properties > General tab. Otherwise the check will fail since it will not know which target to query.

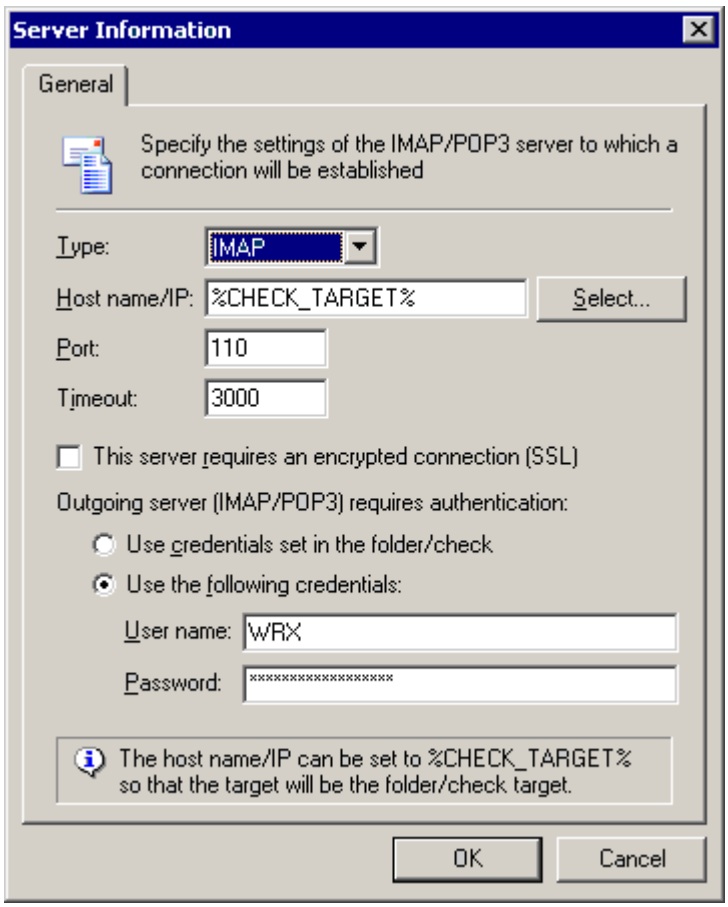
- *Port* - Specify the TCP port through which the connection will be established. The SMTP Port is by default set to 25.
- Timeout – Specify the connection timeout value. This value defines the time interval required for a connection to take place. If the connection is not established within the specified time period, a timed out will occur and an error is generated. By default, this value is set to 3000 milliseconds
- This server requires an encrypted connection (SSL) – Select this option if you want to encrypted the transmission (i.e., establish a secure session by electronically authenticating each end of an encrypted transmission).
- Outgoing server (SMTP) requires authentication – Select this option if your SMTP server requires authentication before the transmission takes place. In addition, you must state the alternative credentials that this check will use by selecting one of the following options:
- Use credentials set in the folder/check – Select this option to use the authentication details specified in the check properties > 'Logon Credentials' tab.

» Use the following credentials – Select this option to specify the additional credentials to be used for authentication (i.e. User name and password).

The New Check Wizard automatically prompts you to configure alternative credentials during the creation of this check. After the check has been created, you can make changes to alternative credentials from the check properties dialog > 'Logon Credentials' tab.

When all required details have been specified, click on 'OK' ' to save and return to the Email Route check properties dialog.

Configuring the POP3/IMAP Server details

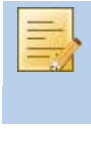


Screenshot 49- POP3/IMAP Server configuration dialog

Click on 'Configure' and specify the following parameters:

» Type – Specify the type of mail server that you want to connect to i.e. POP3 or IMAP.

» Hostname/IP – Specify the name/IP address of the POP3/IMAP server to which this check will connect. By default, this parameter is configured to acquire its value from %CHECK_TARGET% variable. This variable gets its value directly from the Target Computer field in the check properties. If required, specify an alternative target or use the 'Select' button to choose the required POP3/IMAP server from the list of active servers on you network.



When using %CHECK_TARGET%, make sure that you specify the correct Target Computer details (i.e., the name/IP of your POP3/IMAP server) in the check properties > General tab. Otherwise the check will fail since it will not know which target to query.

- Port – Specify the TCP port through which the connection will be established. By default this parameter is set according to the value selected in the 'Type' field (i.e., 995 if POP3 is selected, 993 if IMAP is selected in the 'Type' field). However, you can still specify other port numbers by inputting them directly in the provided field.
- Timeout – Specify the connection timeout value. This value defines the time interval required for a connection to take place. If the connection is not established within the specified time period, a timed out will occur and an error is generated.
- This server requires an encrypted connection (SSL) – Select this option if you want to encrypted the transmission (i.e. establish a secure session by electronically authenticating each end of an encrypted transmission).
- Use credentials set in the folder/check – Select this option to use the authentication details specified in the check properties > 'Logon Credentials' tab.
- Use the following credentials – Select this option to specify additional credentials (i.e. User name and password) for authentication.

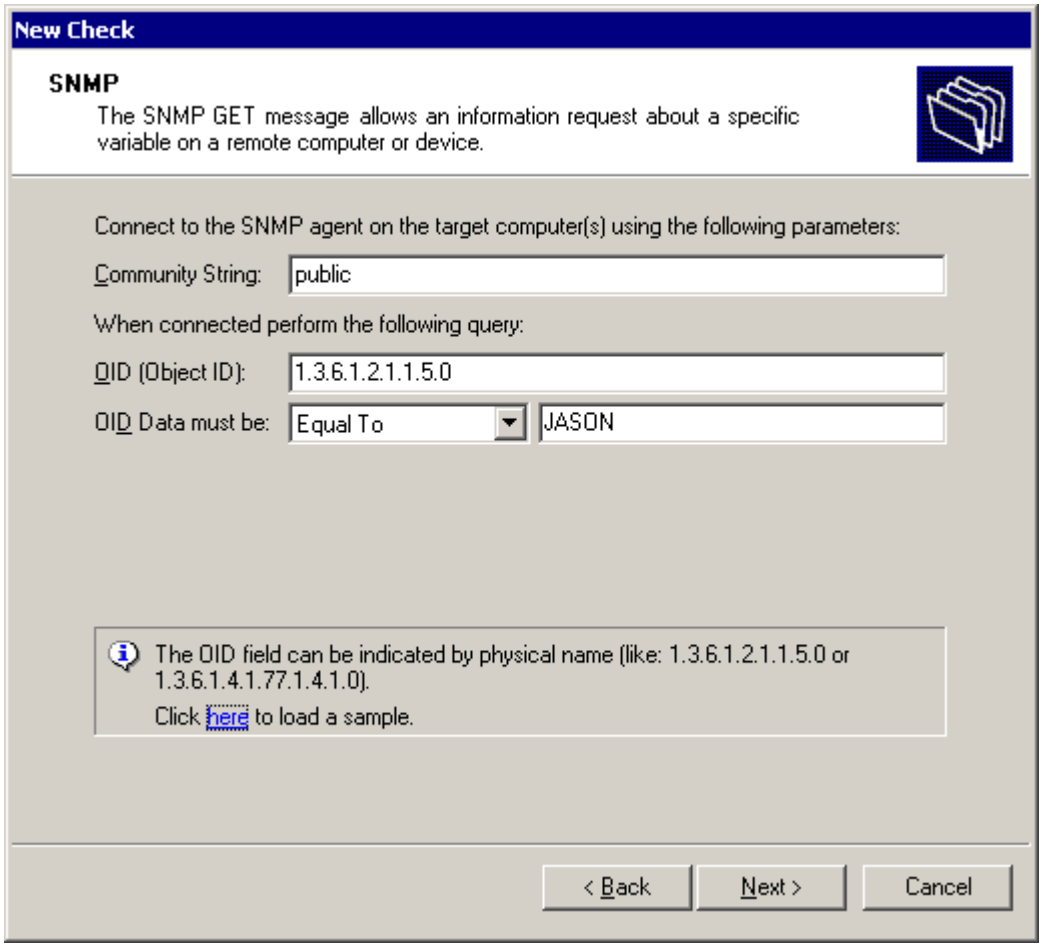
The New Check wizard automatically prompts you to configure alternative credentials during the creation of this check. After the check has been created, you can make changes to alternative credentials from the check properties dialog > 'Logon Credentials' tab.

When all the required details have been specified, click **OK** to save and return to the Email Route check properties dialog.

4.3 SNMP monitoring checks

4.3.1 Generic SNMP function

GFI Network Server Monitor can check local or remote server connections by challenging a specific port. GFI Network Server Monitor carries out this function by connecting to the target computer, send it a sequence of bytes and analyze the response received.


New Check
SNMP
The SNMP GET message allows an information request about a specific variable on a remote computer or device.
Connect to the SNMP agent on the target computer(s) using the following parameters:
Community String:
public
When connected perform the following query:
OID (Object ID):
1.3.6.1.2.1.1.5.0
OID Data must be:
Equal To
JASON
The OID field can be indicated by physical name (like: 1.3.6.1.2.1.1.5.0 or 1.3.6.1.4.1.77.1.4.1.0).
Click here to load a sample.
< Back
Next >
Cancel

Screenshot 50 - SNMP check parameters dialog

The SNMP (Simple Network Management Protocol) GET message allows the Network Monitor Engine to request information about a specific variable on a remote computer or device. Upon receiving a GET message, the agent will issue GFI Network Server Monitor Engine a GET-RESPONSE message containing either the information requested or an error indicating why the request cannot be processed.

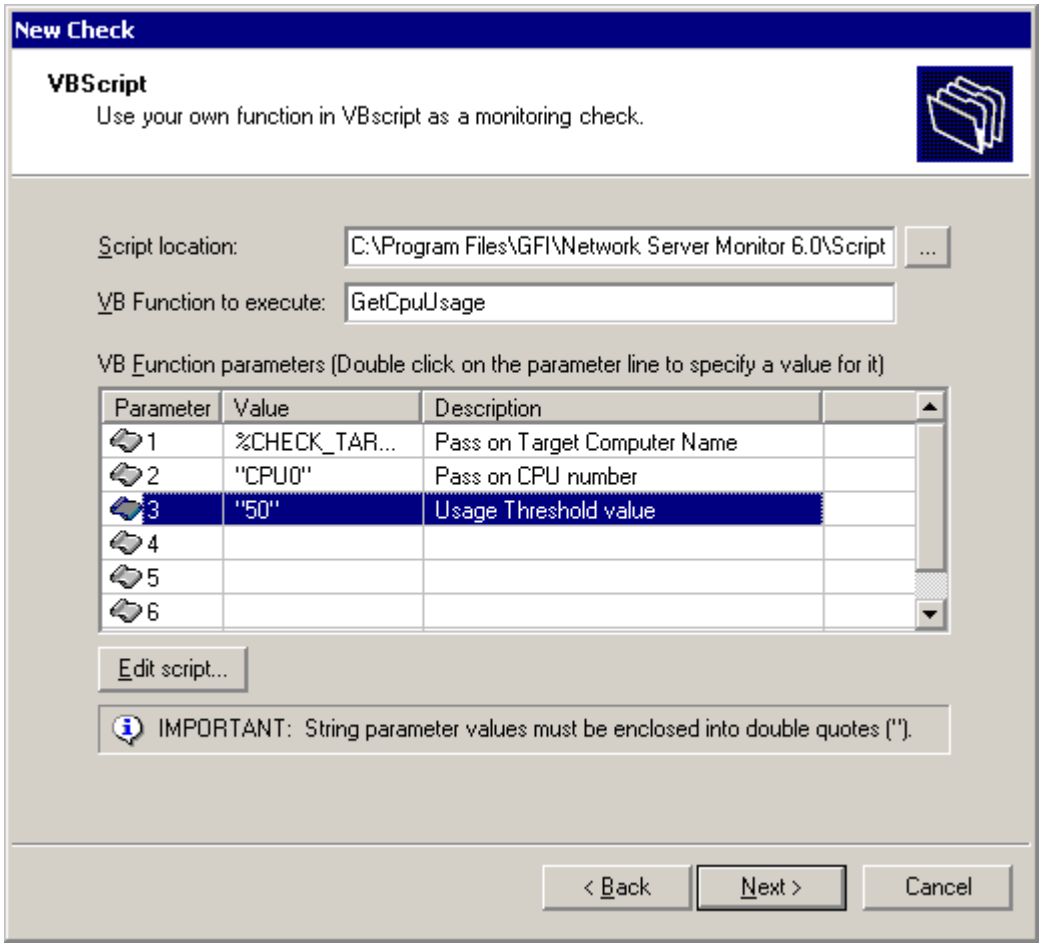
An SNMP function requires the following parameters:

- Community String – Specify the SNMP community string to be used, by default: 'public'.
- OID (Object ID) – Specify the Object ID. This is a unique identification tag, which could be either an alphanumeric name or the physical name (long numeric tag), used to distinguish each variable in SNMP messages.
- OID Data type – Select the data type to be used from the available dropdown list. The following are valid/supported data types: Bit Stream, Counter, Integer, IP address, Object Identifier, Opaque String, String, Time Marks and Unsigned Integer.
- OID Data must be – Specify an OID data value and select the operand to be used to compare the actual SNMP value against the 'IOD Data Value' specified. Supported operands include Equal To, Not Equal To, Less Than, Less or Equal To, Greater Than, Greater or Equal To.

4.4 Windows OS generic checks

4.4.1 Generic VB Script

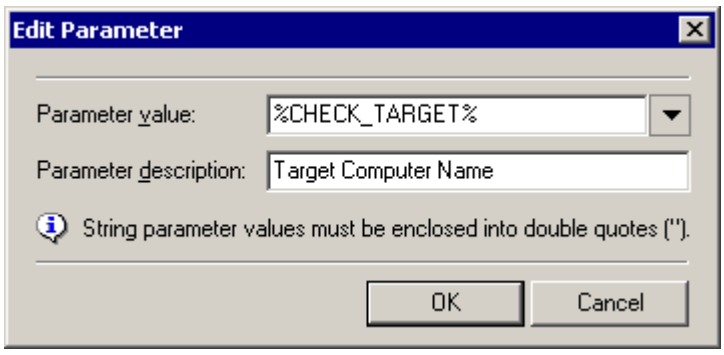
The VBscript function allows you to create custom checks using VBscripts. For more information about writing scripts, please refer to the 'Writing your own monitoring functions' chapter.



Screenshot 51 - VBscript check parameters dialog

A VBScript function requires the following parameters:

- Script location – Specify the path to the required VBScript file. The script should contain the function specified in the Function name field and should return True (-1) in case of success, or False (0) in case of an error.
- Function name – Specify the function that GFI Network Server Monitor service will be calling from the specified script file.



Screenshot 52 - Parameters dialog

- *VB Function Parameters* – In the parameters list, specify any additional parameters required by this function. During check execution these parameters will be automatically passed on to the VB script in the order specified in the VB Function Parameters list. To add a parameter, double click on the position/row where you wish to add this additional parameter and specify the required values in the parameters dialog. Parameter values can be specified as a string, number or can be passed on through system variables (e.g. %USERNAME%).

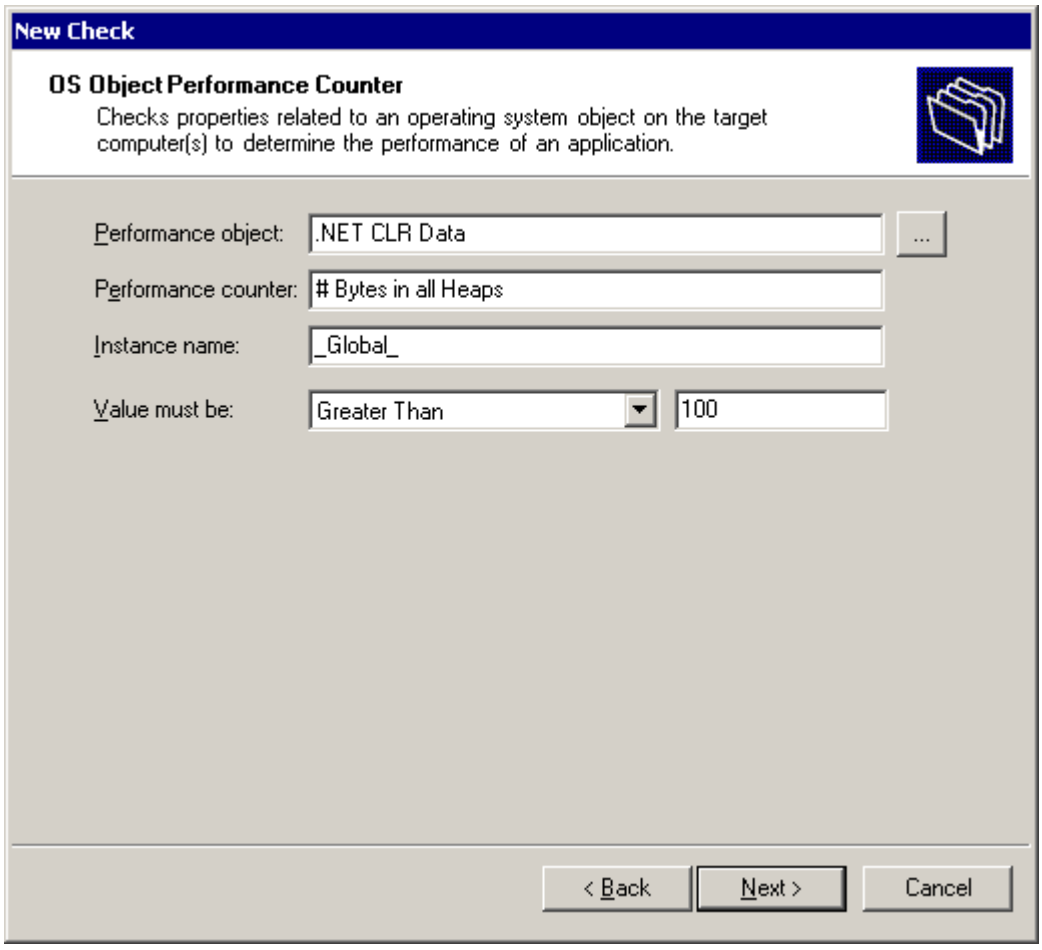
Strings must always be specified within double quotes (“”) e.g. “Mail Server”.

You may make changes to the selected script file by clicking on the ‘Edit script …’ button.

The “Generic Secure Shell (SSH) Check” requires logon credentials (i.e. username and password or Private Key file) to connect (authenticate) and run SSH scripts on a remote Unix-based target computer. These credentials must be specified from the ‘Logon Credentials’ tab available in the properties of the relative check. For more information on logon credentials, please refer to the ‘Logon credentials’ section in the ‘Configuring GFI Network Server Monitor’ chapter.

4.4.2 OS Object Performance Counter

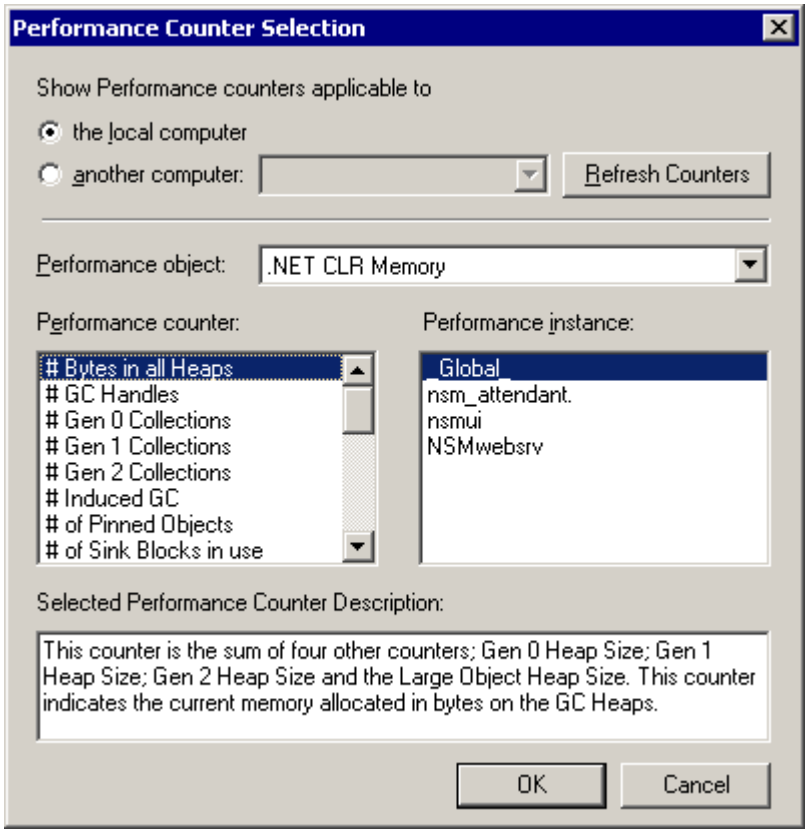
The OS Object Performance Counter establishes the performance of an operating system object available on the target computer by checking its properties.



Screenshot 53 - OS Object Performance Counter check parameters dialog

The parameters required for this function are:

Performance Object - Click on the ... button to display the list of available objects.


Performance Counter Selection
Show Performance counters applicable to
the local computer
another computer:
Refresh Counters
Performance object:
.NET CLR Memory
Performance counter:
Performance instance:
Bytes in all Heaps
GC Handles
Gen 0 Collections
Gen 1 Collections
Gen 2 Collections
Induced GC
of Pinned Objects
# of Sink Blocks in use
Global
nsm_attendant.
nsmui
NSMwebsrv
Selected Performance Counter Description:
This counter is the sum of four other counters; Gen 0 Heap Size; Gen 1 Heap Size; Gen 2 Heap Size and the Large Object Heap Size. This counter indicates the current memory allocated in bytes on the GC Heaps.
OK
Cancel

Screenshot 54 - Performance Counter - Object Selection Dialog

1. Specify the target computer containing the object/performance counters that need to be shown by selecting one of the following options:

- Select 'this computer' to use the performance counters available on the target computer.
- Select 'another computer' and specify the computer name to use performance counters available on another computer.

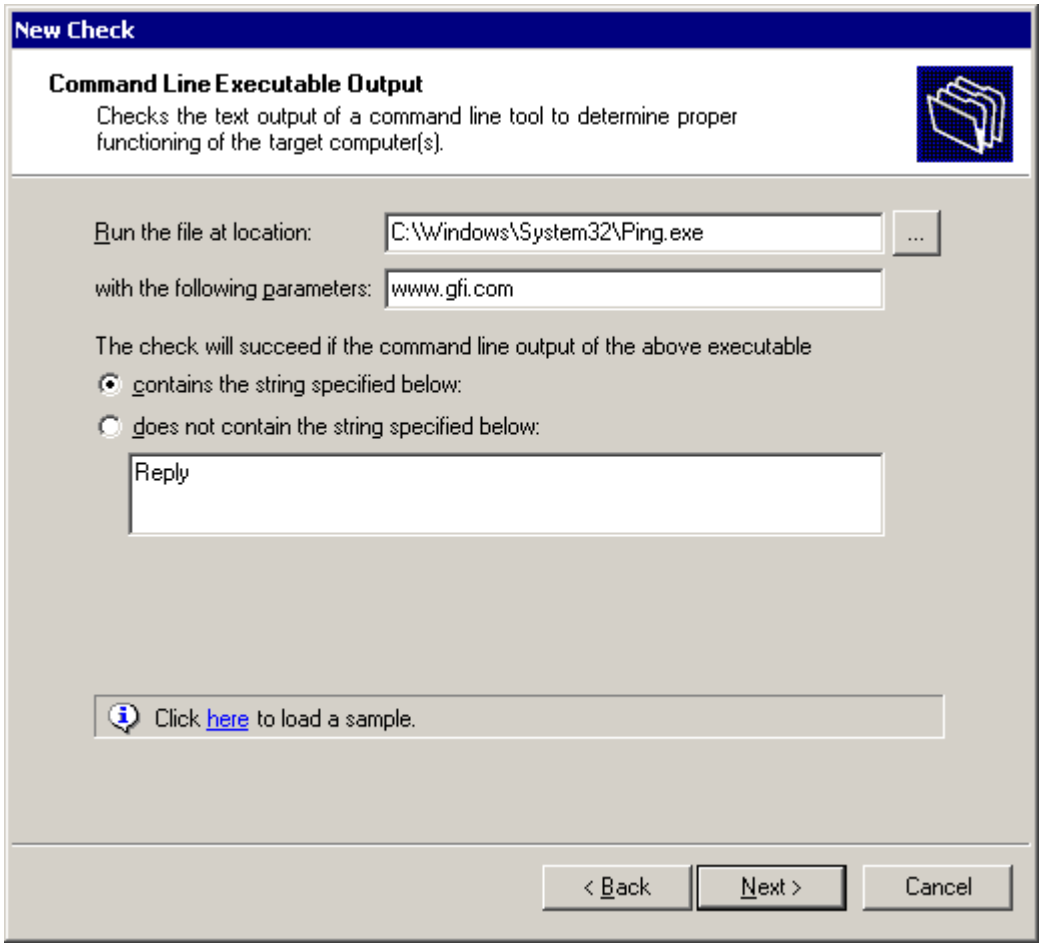
2. Select from the available dropdown list, the Object to be checked. (e.g. Select 'Memory' to check the memory performance of the specified computer).

3. Select the Performance Counter to be used. (e.g. Available bytes – should determine the amount of physical memory in bytes available for system use / process allocation).

- *Value* must be – Select the operand that will be used for comparing the Performance Counter value to the comparison value specified.
- Comparison Value – Specify the value with which the performance counter value will be compared.

4.4.3 Command Line executable output

This function checks the text output of a command line tool / application in order to determine if it is functioning correctly.


New Check
Command Line Executable Output
Checks the text output of a command line tool to determine proper functioning of the target computer(s).
Run the file at location:
C:\Windows\System32\Ping.exe
...
with the following parameters:
www.gfi.com
The check will succeed if the command line output of the above executable
contains the string specified below:
does not contain the string specified below:
Reply
Click here to load a sample.
< Back
Next >
Cancel

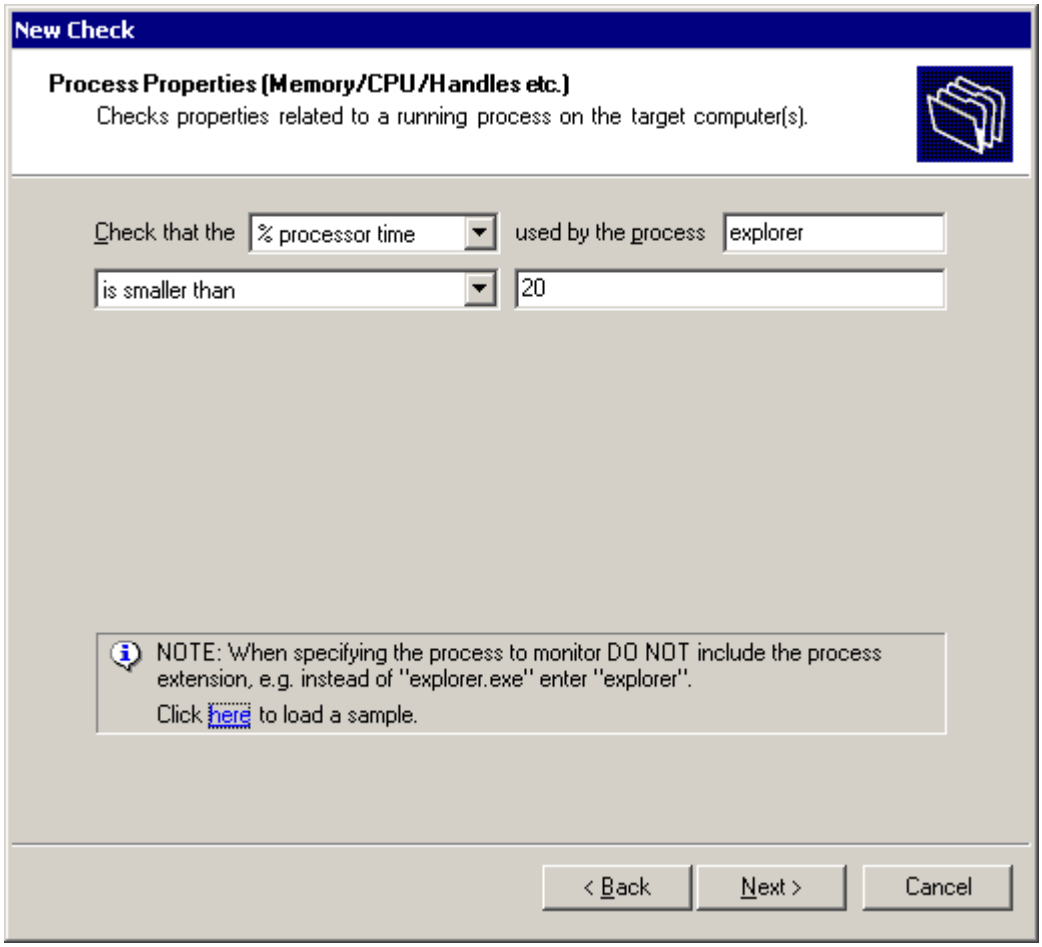
Screenshot 55 - Command Line Output check parameters dialog

The parameters required for this function are:

- *Run the file at location* – Specify the complete path to the command line tool file which must be executed (e.g.C:\Windows\System32\Ping.exe).
- With the following parameters – Specify additional parameters required by the specified tool (e.g. the IP address / name of host to which the ping will be sent).
- Contains the following text – Enable this flag and specify the string to be searched in the command line output. If a matching string is found, the check will be classified as successful.
- Does not contain the following string – Enable this flag and specify the string to be searched for, in the command line output. In this case, if no matching string is found the check is classified as successful.

4.4.4 Process Properties (Memory/CPU/Handles etc.)

This function checks for properties related to a process running on specified target computers. Such checks include % processor usage, % user time consumed, % privileged time consumed, number of handles, number of threads, physical memory and virtual memory in use by application.


New Check
Process Properties (Memory/CPU/Handles etc.)
Checks properties related to a running process on the target computer(s).
Check that the
% processor time
used by the process
explorer
is smaller than
20
NOTE: When specifying the process to monitor DO NOT include the process extension, e.g. instead of "explorer.exe" enter "explorer".
Click here to load a sample.
< Back
Next >
Cancel

Screenshot 56 - Process Properties check parameters dialog

The parameters required for this function include:

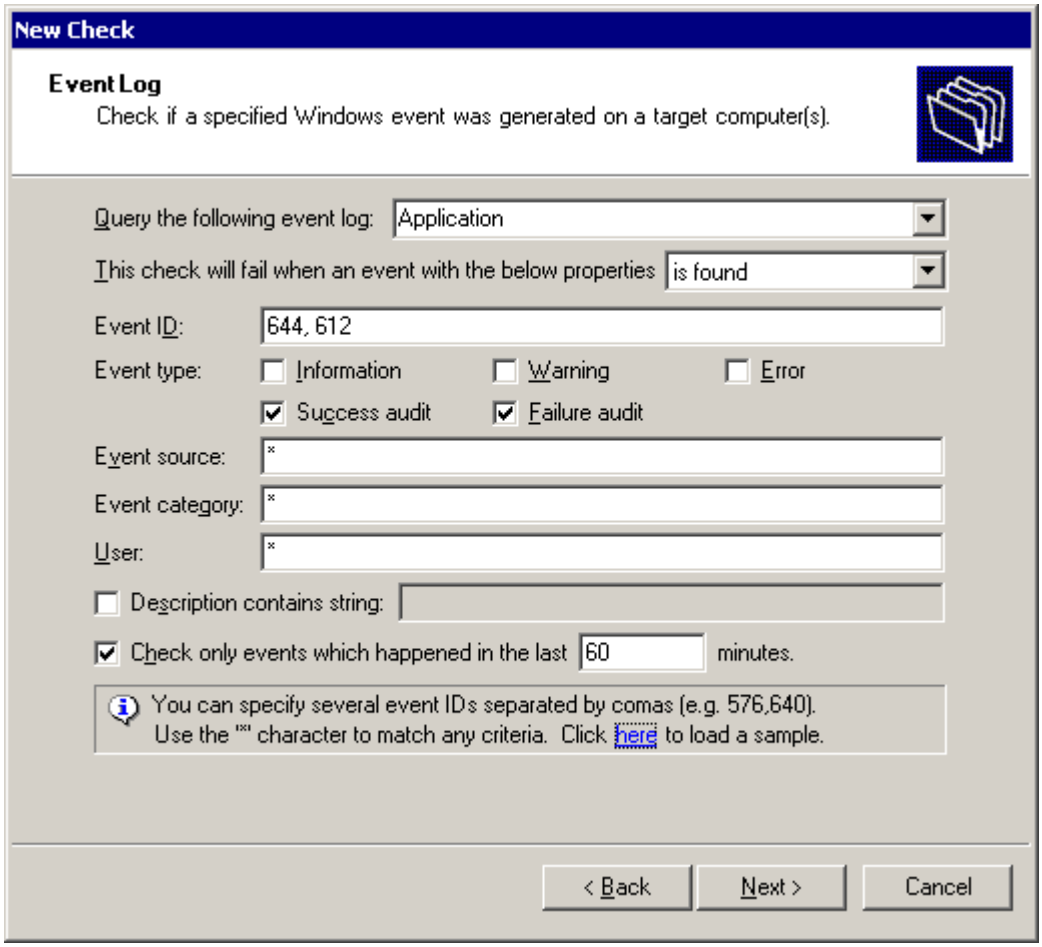
- Check that the…. – Select the system resource that will be checked from the dropdown list.
- Used by the process – Specify the name of the process to be checked.
- Operand – Select the operand and specify the value to be compared with the result.

4.5 Windows operating system checks

4.5.1 Event Log

This monitor function requires WMI to be installed on the computer running GFI Network Server Monitor as well as on the computer being monitored. The monitor function will create a VBscript, which uses WMI, with the parameters you specify in the check parameters dialog. WMI is only available on Windows 2000 and higher computers, so this monitor function can only be used if both the GFI Network Server Monitor computer and the computer to be monitored are running Windows 2000 or higher.

GFI Network Server Monitor can read Windows Event logs on local or remote computers and can search their contents for specific Event Sources, Categories, Event ID's, etc..



Screenshot 57 - Event log check parameters dialog

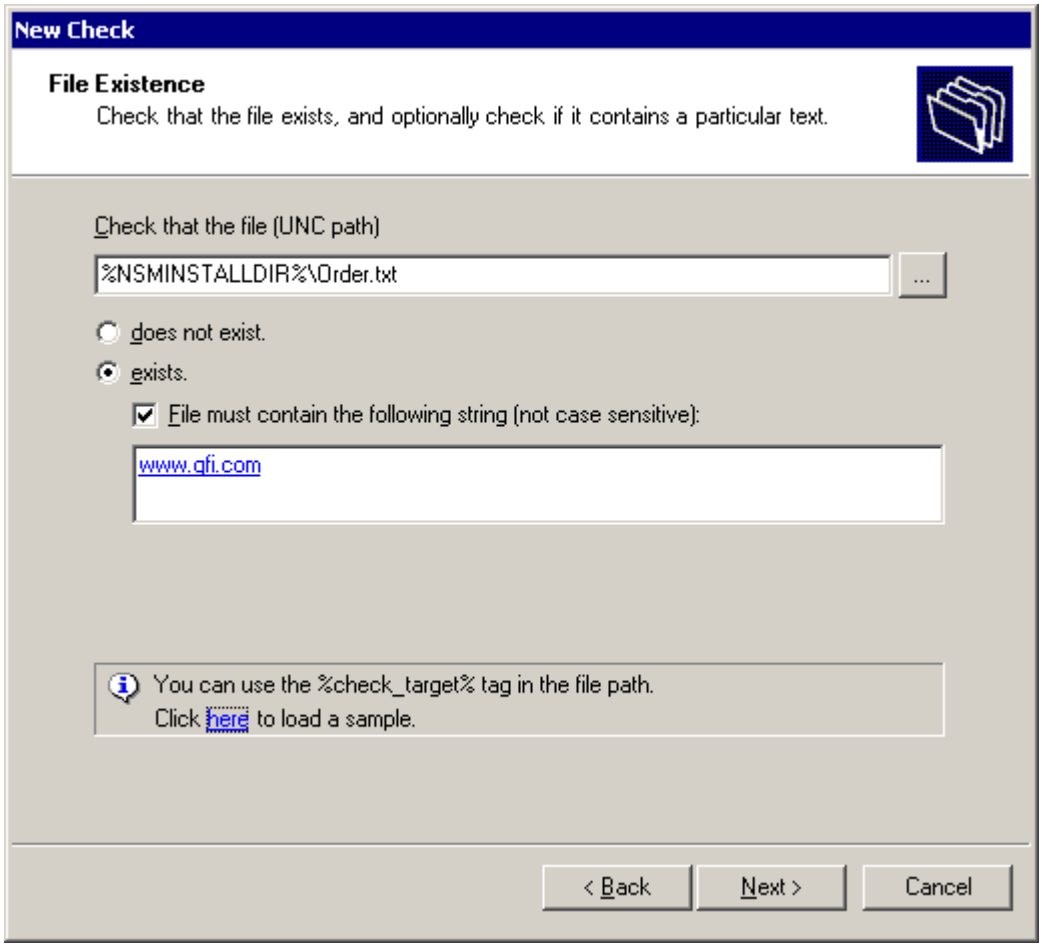
It can also look for specific patterns in the description of an event as well as notify the system administrator if one of the events occurred within a specific period of time (e.g. You can check if a message from your antivirus software has been posted in the Application Event Log during the last 30 minutes. An Event Log function requires the following parameters:

- Query the following event Log – Select the log File to be checked, from the dropdown list. Available logs include 'Application', 'Security', 'System', or server-related log (like DNS, Exchange, etc).
- This check will fail when … – Specify whether this check will fail when an event having the specified properties is found or vice versa.
- Event ID – Specify an event ID. GFI Network Server Monitor will filter events that match the specified ID (i.e. filter events by ID).
- Event Type – Enable the event types that will be filtered and checked from the event logs (i.e. filter events by type e.g. enable 'Warning' to check and filter warning logs only).
- Event Source – Specify event sources that must be filtered from the logs (i.e. filter events by source).
- Event Category – Specify event categories that must be filtered from the log (i.e. filter events by category).
- User – Specify the name of the user whose events are to be filtered (i.e. filter events by user).
- Description contains string – Specify the string to search for, in the file contents (i.e. filter event by content string).
- Check only events which happened in the last x minutes – Specify this value to filter events occurring during the specified period of time (i.e. filter events by time of occurrence).

Use (*) wildcard to indicate all/any criteria.

4.5.2 File Existence

GFI Network Server Monitor can check for the existence of a particular file on a target computer as well as search its contents for particular strings. This is particularly convenient when checking for results of scheduled batch jobs and other logging information.


New Check
File Existence
Check that the file exists, and optionally check if it contains a particular text.
Check that the file (UNC path)
%NSMINSTALLDIR%\Order.txt
...
does not exist.
exists.
File must contain the following string (not case sensitive):
www.gfi.com
You can use the %check_target% tag in the file path.
Click here to load a sample.
< Back
Next >
Cancel

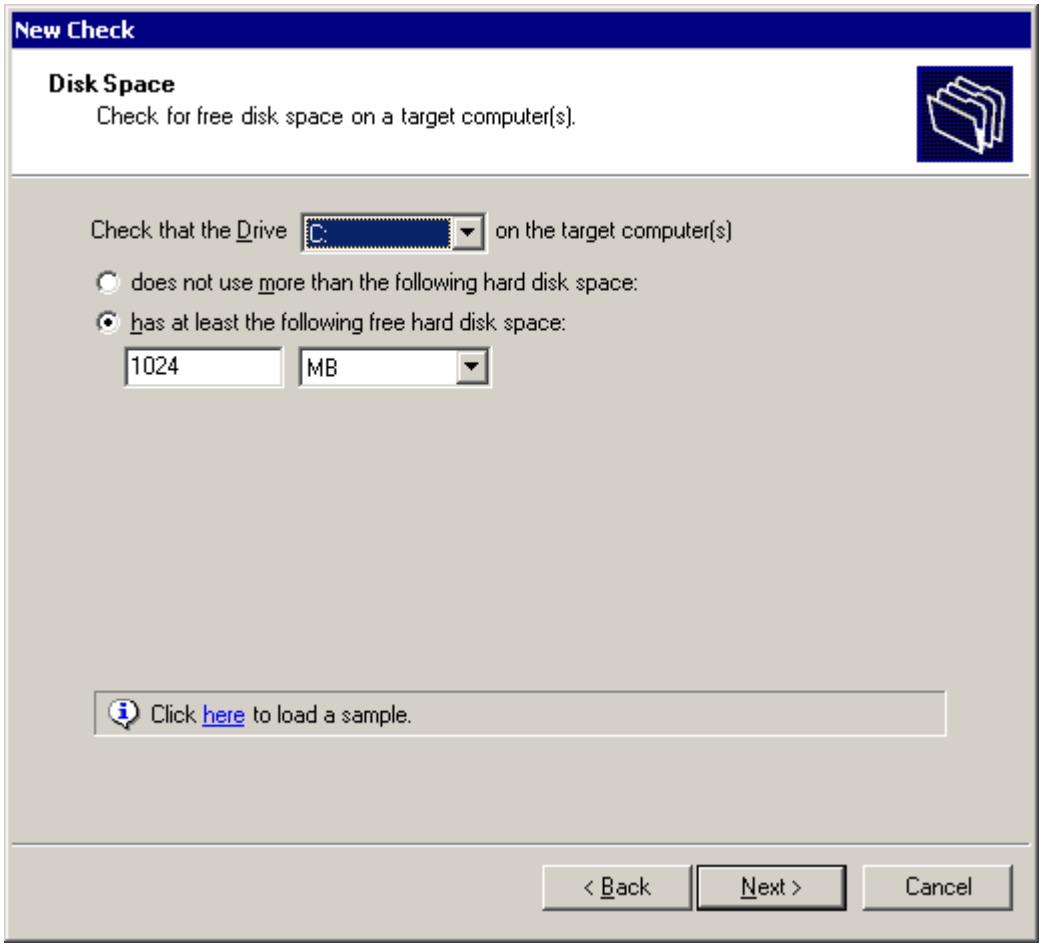
Screenshot 58 - File existence check parameters dialog

A File Existence function requires the following parameters:

- File (UNC Path) – Specify the path to the file which is to be checked in UNC format (e.g. \\server\share\today_job_results.txt).
- Does not exist – Enable this option to check if the file exists. In this case, the check fails if the specified file is found.
- Exists - Enable this option to check if the file exists. In this case, the check succeeds if the specified file is found.
- File must contain …string – Enable this flag and specify the string to be searched for in the existing file contents. In this case the check will succeed only if the file exists and the specified string is present in the file contents.

4.5.3 Disk Space

GFI Network Server Monitor can check for free disk space on local and remote computers. Alerts can be sent whenever hard disk space falls below a specified value in order for you to take proactive actions before running out of disk space.


New Check
Disk Space
Check for free disk space on a target computer(s).
Check that the Drive C: on the target computer(s)
does not use more than the following hard disk space:
has at least the following free hard disk space:
1024
MB
Click here to load a sample.
< Back
Next >
Cancel

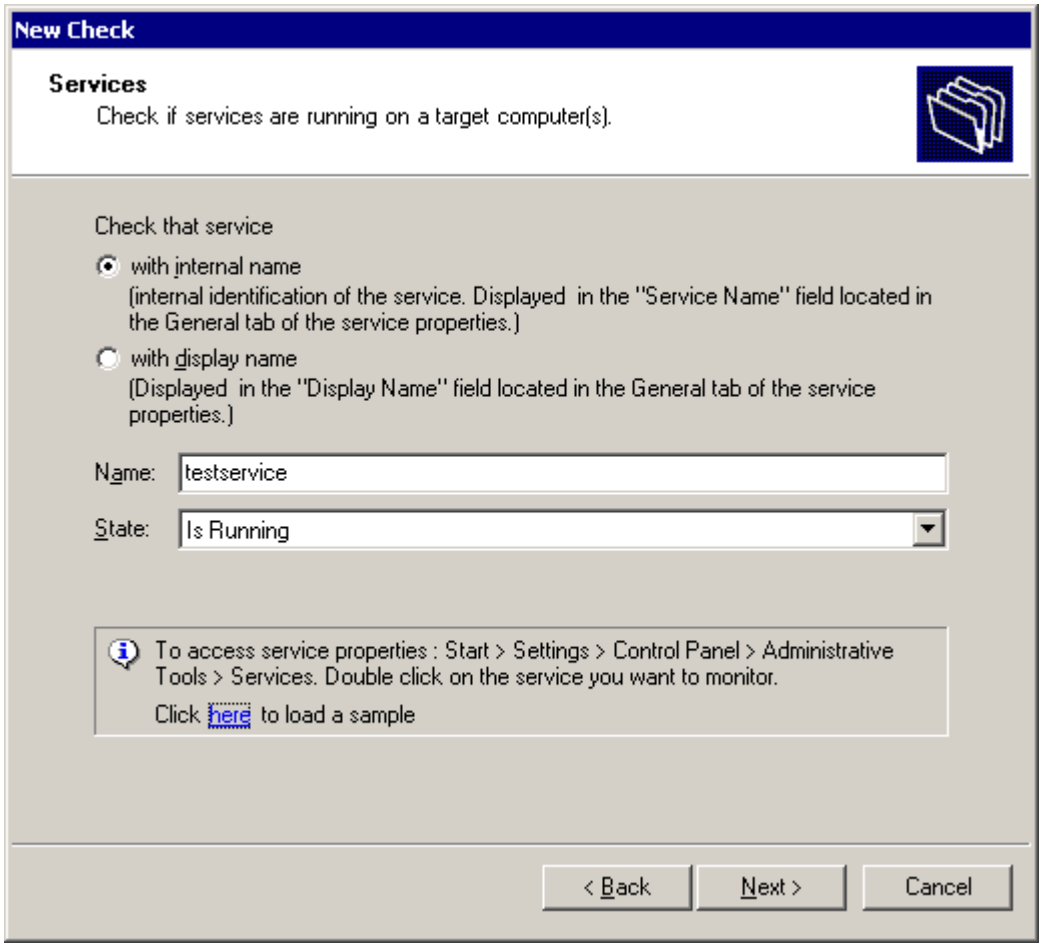
Screenshot 59 - Disk space check parameters dialog

A Disk Space function requires the following parameters:

- Check that the Drive… – Select the disk drive to be checked.
- Does not use more than the following hard disk space – Enable this option and specify the maximum disk space that can be used. The monitoring check will fail if the specified disk limit is exceeded.
- Has at least the following free hard disk space – Enable this option and specify the minimum amount of free disk space required on the target computer. The monitoring check will fail when disk space is below the specified (minimum) value.

4.5.4 Services

GFI Network Server Monitor can monitor services on local and remote computers by checking if their status equals to "Running".


New Check
Services
Check if services are running on a target computer(s).
Check that service
with internal name
(internal identification of the service. Displayed in the "Service Name" field located in the General tab of the service properties.)
with display name
(Displayed in the "Display Name" field located in the General tab of the service properties.)
Name:
testservice
State:
Is Running
To access service properties : Start > Settings > Control Panel > Administrative Tools > Services. Double click on the service you want to monitor.
Click here to load a sample
< Back
Next >
Cancel

Screenshot 60 - Services check parameters dialog

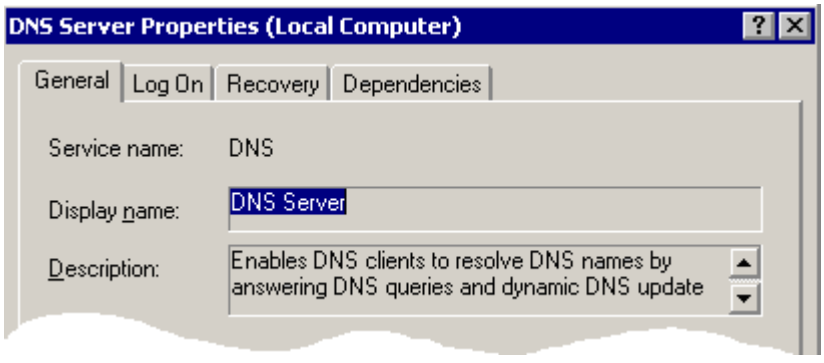
A Service monitor function requires the following parameters:

- With internal name – Enable this option to check for services having an internal identification / name identical to the string specified in the NAME field. The Internal identification is the 'Service Name' displayed in the General dialog of the service properties.
- With display name – Enable this option to check for services having a display name identical to the string specified in the NAME field. The display name can be seen in the General dialog of the service properties.

To view the internal and display name of a service:

1. Go on Start > Programs > Administrative Tools > Services.

2. Double click on the service to open the properties dialog. The Service and Display names are shown in the general dialog.

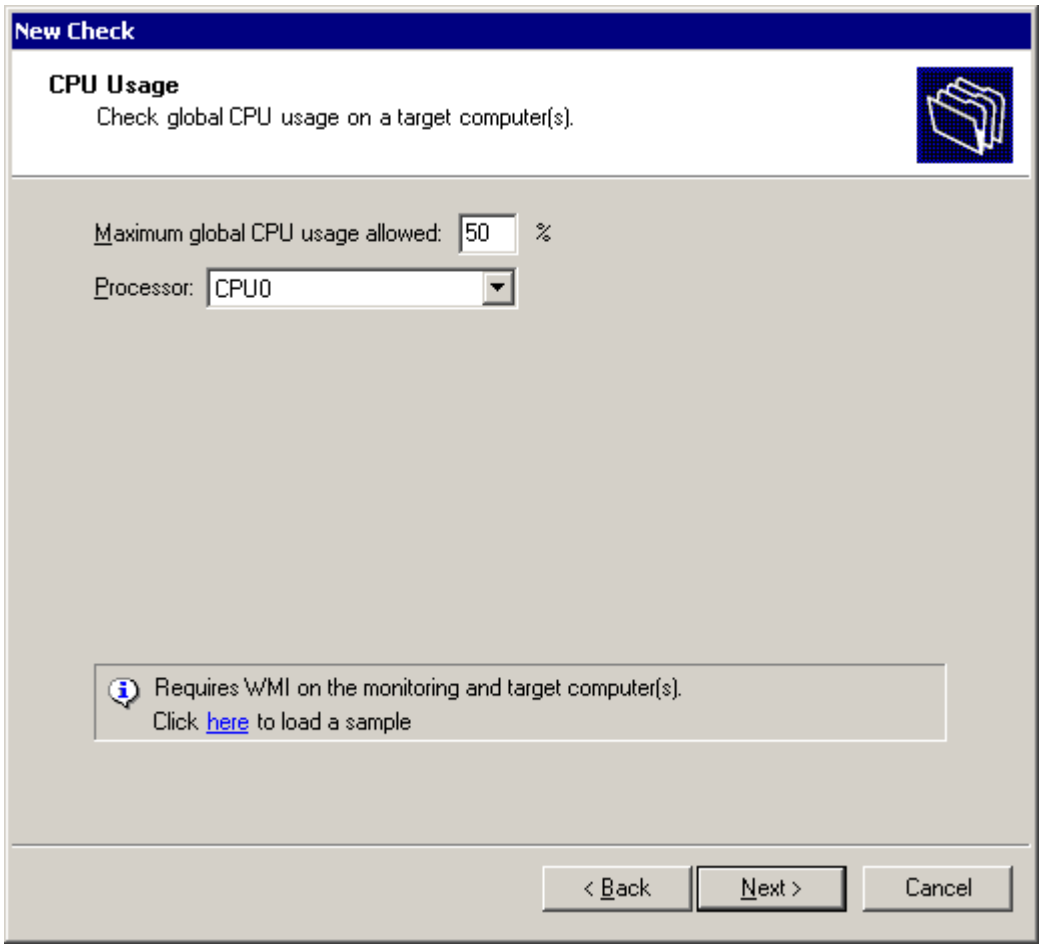


Screenshot 61 - DNS Server Service and display name

4.5.5 CPU Usage

This monitor function requires WMI to be installed on the computer running GFI Network Server Monitor as well as on the computer being monitored. The monitor function will create a VBscript which uses WMI with the parameters you specify in the check parameters dialog. WMI is only available on Windows 2000 and higher computers, therefore this monitor function can only be used if both the GFI Network Server Monitor computer and the computer to be monitored are running Windows 2000 or higher.

GFI Network Server Monitor can check the processor usage status on Windows based target computers. You can setup alerts and trigger other actions (e.g. run an external file) whenever the load of a specific processor exceeds the maximum usage allowed.



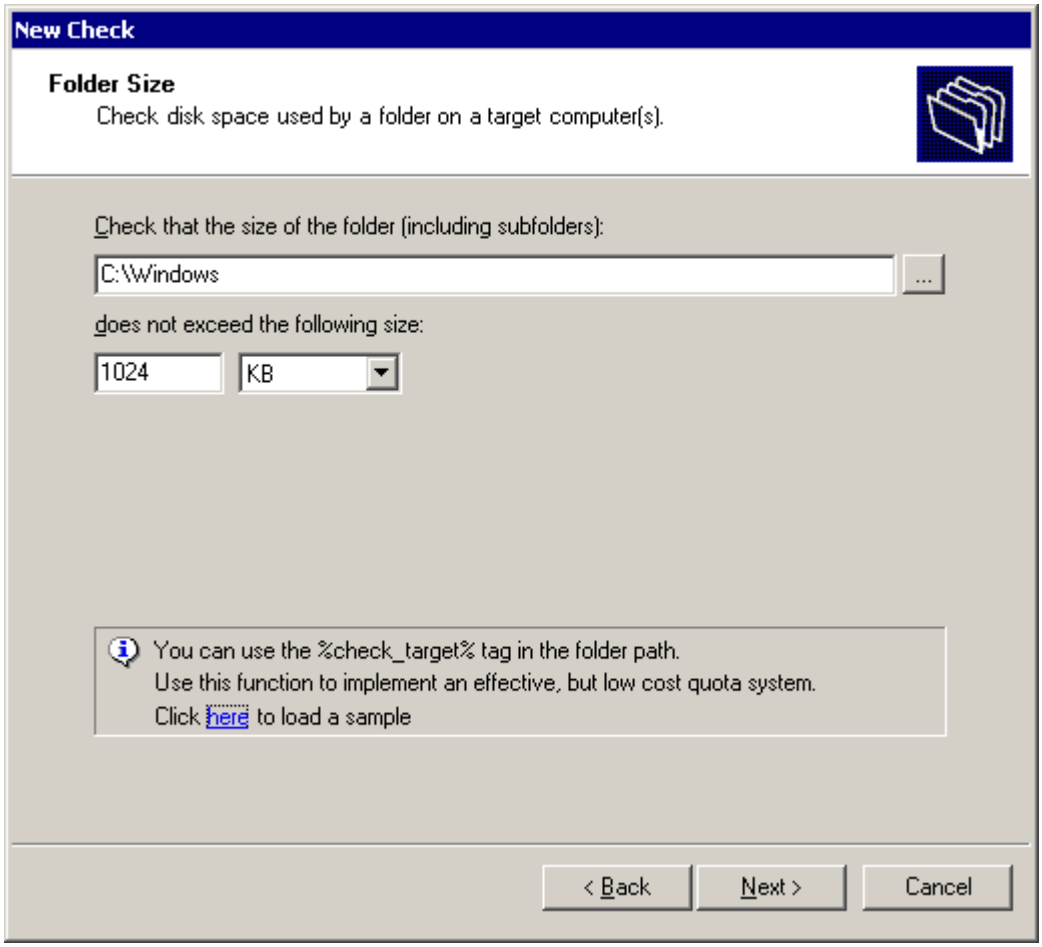
Screenshot 62 - CPU usage check parameters dialog

A CPU Usage function requires the following parameters:

- Maximum global CPU usage allowed – Specify the (maximum) % CPU usage allowed on the target computer.
- Processor – Specify which CPU will be checked. CPU0 is the default value for computers having one processor.

4.5.6 Directory/Folder Size

GFI Network Server Monitor can check the disk space used by a directory / folder on target computers. You can use this function to implement a disk control / quota system, which notifies you when a specific folder exceeds the maximum size specified.


New Check
Folder Size
Check disk space used by a folder on a target computer(s).
Check that the size of the folder (including subfolders):
C:\Windows
...
does not exceed the following size:
1024
KB
You can use the %check_target% tag in the folder path.
Use this function to implement an effective, but low cost quota system.
Click here to load a sample
< Back
Next >
Cancel

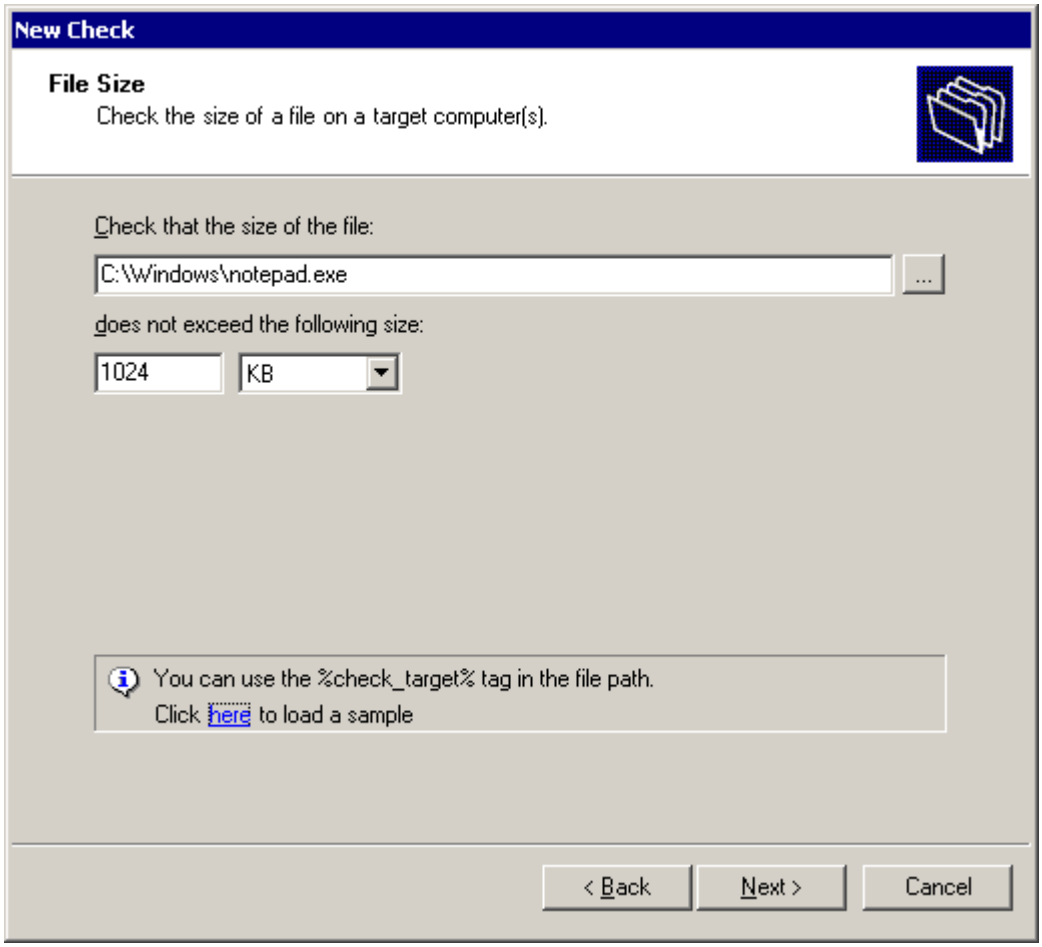
Screenshot 63 - Directory Size check parameters dialog

The Directory Size function requires the following parameters:

- Directory Name – Specify the path to the folder/directory in UNC format (e.g. \\server01\public\docs) which needs to be monitored.
- Directory size limit – Specify the maximum size in KB, MB or GB allowed for this directory.

4.5.7 File Size

GFI Network Server Monitor can check for the size of particular files on local and remote computers. You can use this function to monitor the size of files (e.g., Outlook .pst files) and generate alerts whenever these files reach or exceed the specified size.


New Check
File Size
Check the size of a file on a target computer(s).
Check that the size of the file:
C:\Windows\notepad.exe
...
does not exceed the following size:
1024
KB
You can use the %check_target% tag in the file path.
Click here to load a sample
< Back
Next >
Cancel

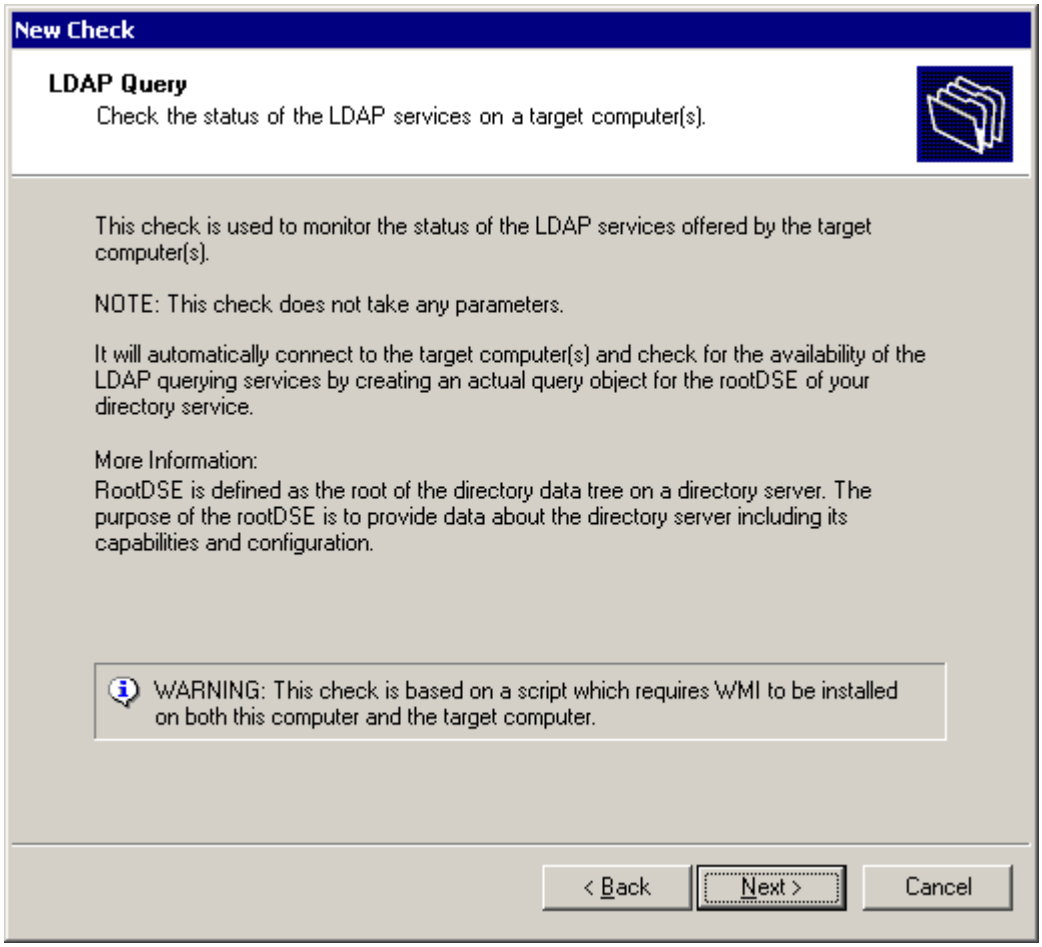
Screenshot 64 - File size check parameters dialog

The file size function requires the following parameters:

- File name – Specify the path to the file in UNC format (e.g. \\server01\public\docs.txt) which needs to be monitored.
- File size limit – Specify the maximum size in KB, MB or GB allowed for this file.

4.5.8 LDAP query

GFI Network server monitor can verify if LDAP Services are available on target computers by querying the rootDSE for the relative information.


New Check
LDAP Query
Check the status of the LDAP services on a target computer(s).
This check is used to monitor the status of the LDAP services offered by the target computer(s).
NOTE: This check does not take any parameters.
It will automatically connect to the target computer(s) and check for the availability of the LDAP querying services by creating an actual query object for the rootDSE of your directory service.
More Information:
RootDSE is defined as the root of the directory data tree on a directory server. The purpose of the rootDSE is to provide data about the directory server including its capabilities and configuration.
WARNING: This check is based on a script which requires WMI to be installed on both this computer and the target computer.
< Back
Next >
Cancel

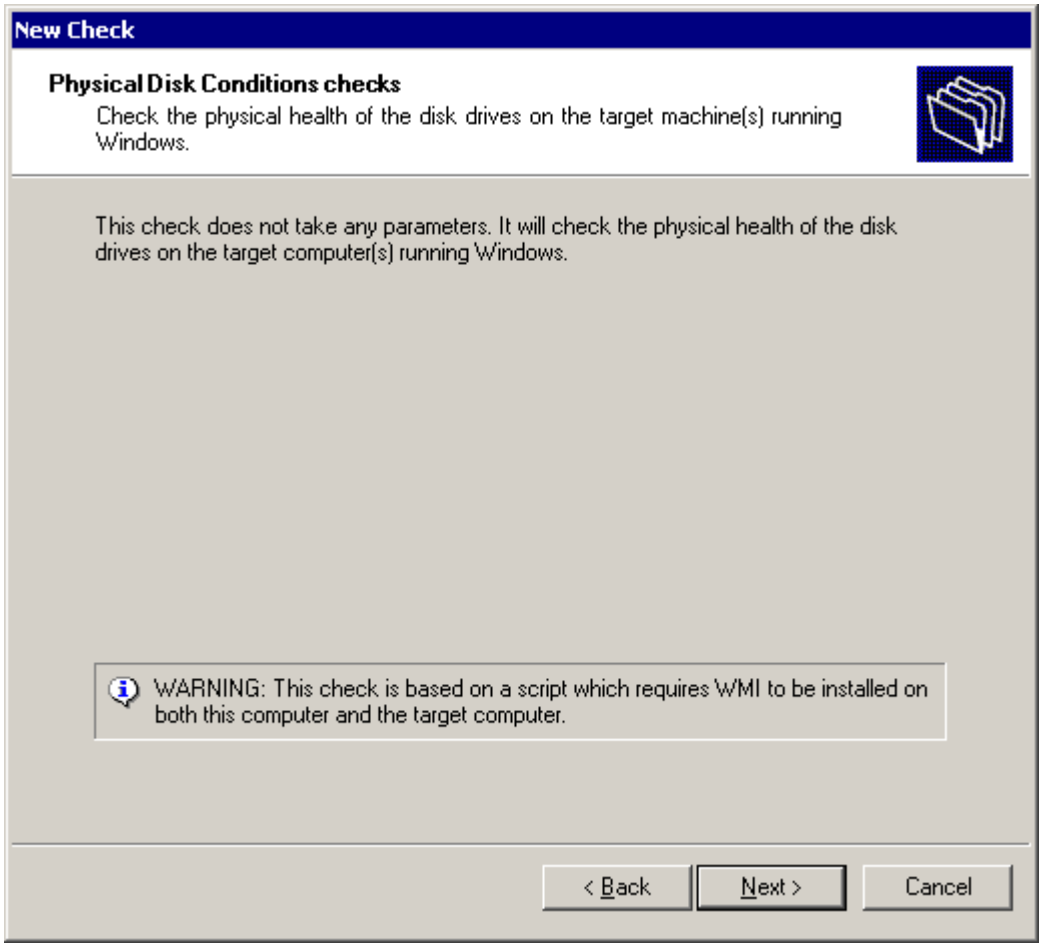
Screenshot 65 - LDAP Query check parameters dialog

No Setup parameters are required for this check.

4.5.9 Physical disk conditions check

This monitor function requires WMI to be installed on the computer running GFI Network Server Monitor as well as on the computer being monitored.

GFI Network server monitor can check the physical condition of the disk drives mounted on computers running windows operating systems.


New Check
Physical Disk Conditions checks
Check the physical health of the disk drives on the target machine(s) running Windows.
This check does not take any parameters. It will check the physical health of the disk drives on the target computer(s) running Windows.
WARNING: This check is based on a script which requires WMI to be installed on both this computer and the target computer.
< Back
Next >
Cancel

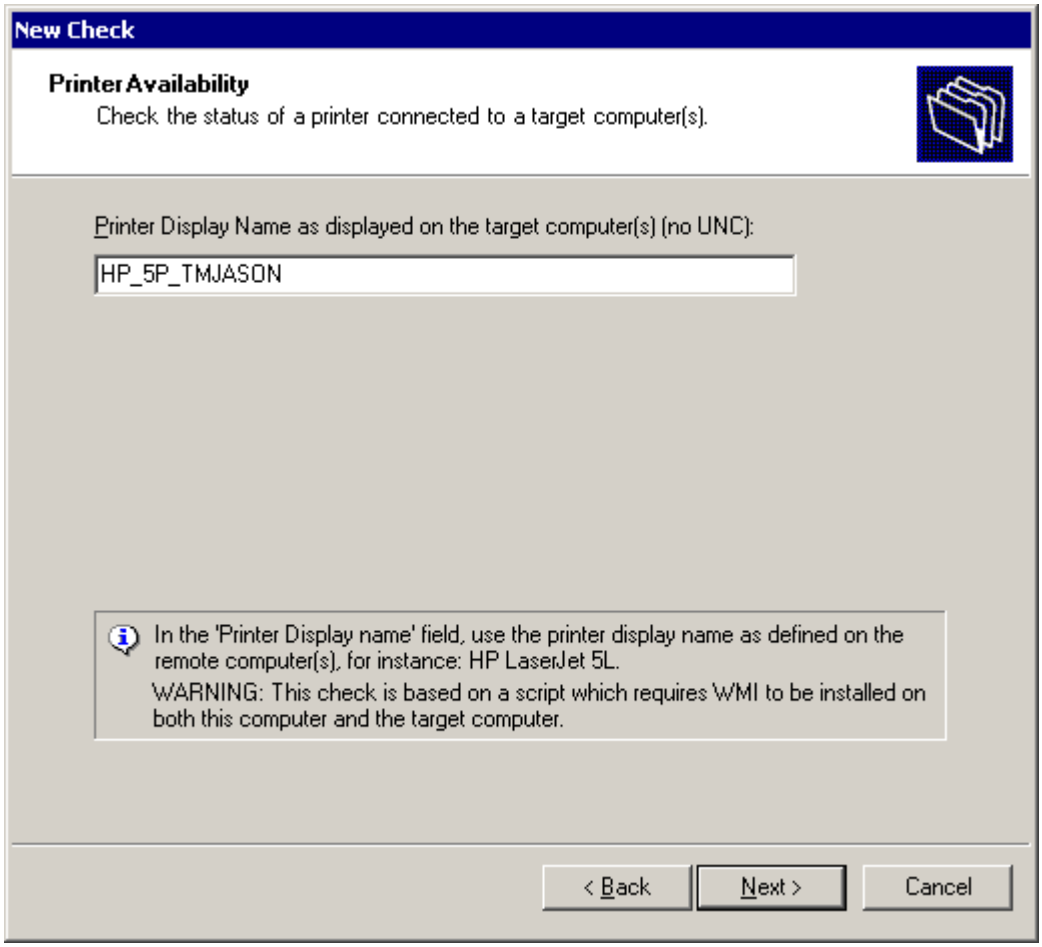
Screenshot 66 - Physical Disk check parameters dialog

No parameters are required for this function.

4.5.10 Printer availability

GFI Network Server Monitor monitors the availability of network printers by checking their status definition. Supported status definitions include *'Running', 'In Test', 'Power Off', 'Offline', and 'Power Save'*. If the Printer Status is not equal to '*Running'* or '*Power Save'*, then GFI Network Server Monitor will consider this printer as being down. You can configure this function to send alerts to the recipients concerned, whenever a printer is down.

To run this check, you must configure the printers to be monitored as network printers on the target computer.


New Check
Printer Availability
Check the status of a printer connected to a target computer(s).
Printer Display Name as displayed on the target computer(s) (no UNC):
HP_5P_TMJASON
In the 'Printer Display name' field, use the printer display name as defined on the remote computer(s), for instance: HP LaserJet 5L.
WARNING: This check is based on a script which requires WMI to be installed on both this computer and the target computer.
< Back
Next >
Cancel

Screenshot 67 - Printer availability check parameters dialog

The Printer Availability rule requires the following parameter:

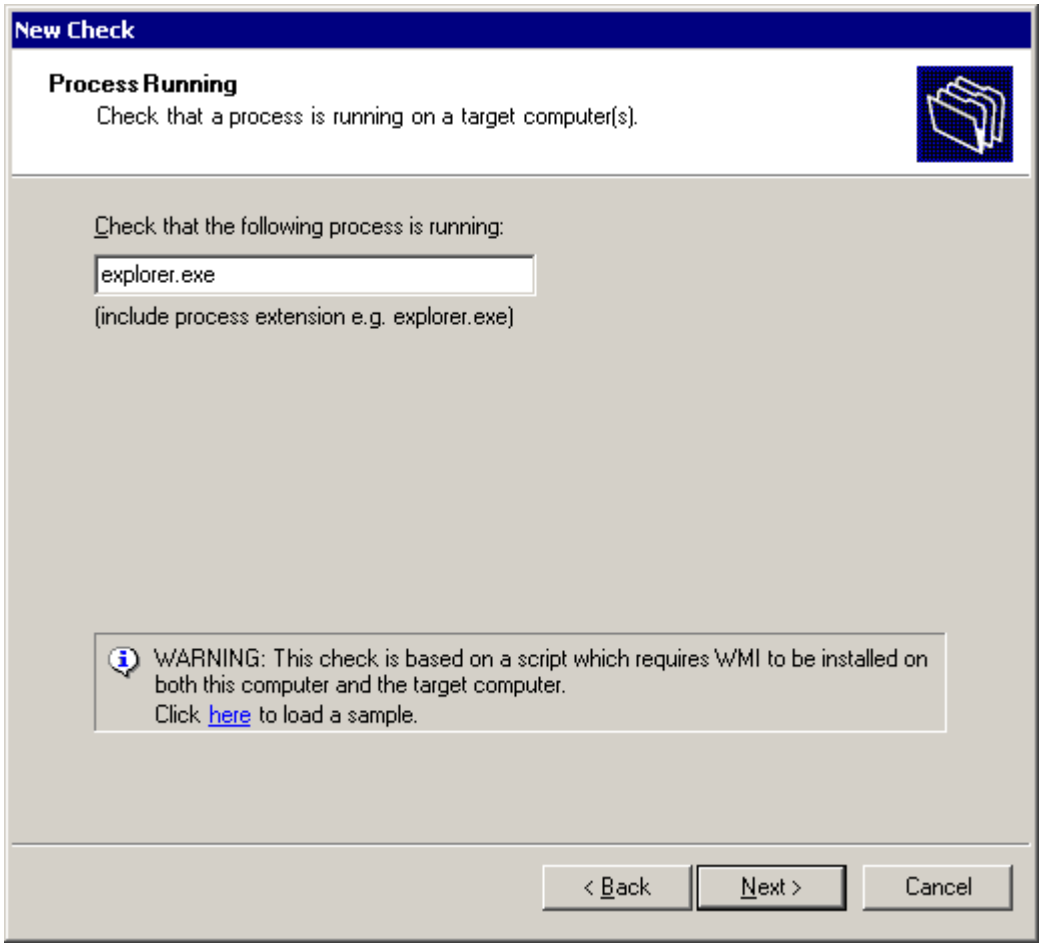
» *Printer name* – Specify the name of the network printer to be monitored.

Specify the same printer name used on the network (e.g. HP4P_onJMPC).

4.5.11 Process Running

This monitor function requires WMI to be installed on the computer running GFI Network Server Monitor as well as on the computer being monitored. The monitor function will create a VBscript which uses WMI with the parameters you specify in the check parameters dialog. WMI is only available on Windows 2000 and higher computers, therefore this monitor function can only be used if both the GFI Network Server Monitor computer and the computer to be monitored are running Windows 2000 or higher.

GFI Network Server Monitor can check for processes running on local and/or remote computers. If a process is active, then the target computer is considered to be available.


New Check
Process Running
Check that a process is running on a target computer(s).
Check that the following process is running:
explorer.exe
(include process extension e.g. explorer.exe)
WARNING: This check is based on a script which requires WMI to be installed on both this computer and the target computer.
Click here to load a sample.
< Back
Next >
Cancel

Screenshot 68 - Running Process check parameters dialog

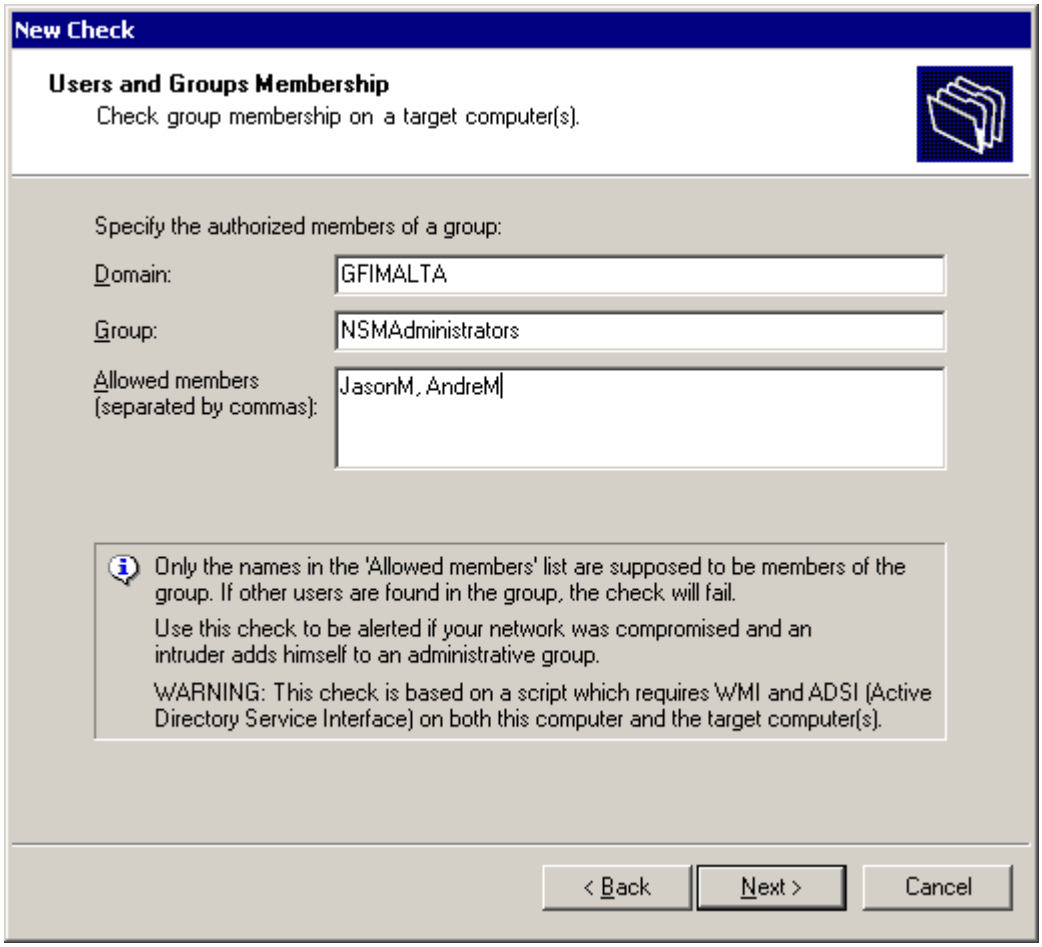
A Process monitor rule requires the following parameter:

- *Process* – Specify the module name of the process which needs to be monitored. For instance: alerter.exe, or explorer.exe.

4.5.12 Users and Group membership

This monitor function requires WMI to be installed on the computer running GFI Network Server Monitor as well as on the computer being monitored. The monitor function will create a VBscript which uses WMI with the parameters you specify in the check parameters dialog. WMI is only available on Windows 2000 and higher computers, therefore this monitor function can only be used if both the GFI Network Server Monitor computer and the computer to be monitored are running Windows 2000 or higher.

GFI Network Server Monitor checks groups and group memberships for unexpected/unauthorised members which could make your system vulnerable to attacks (e.g. intruders in the Domain Admins group).


New Check
Users and Groups Membership
Check group membership on a target computer(s).
Specify the authorized members of a group:
Domain:
GFIMALTA
Group:
NSMAdministrators
Allowed members (separated by commas):
JasonM, AndreM
Only the names in the 'Allowed members' list are supposed to be members of the group. If other users are found in the group, the check will fail.
Use this check to be alerted if your network was compromised and an intruder adds himself to an administrative group.
WARNING: This check is based on a script which requires WMI and ADSI (Active Directory Service Interface) on both this computer and the target computer(s).
< Back
Next >
Cancel

Screenshot 69 - Users and Groups check parameters dialog

The User and Groups membership function requires the following parameters:

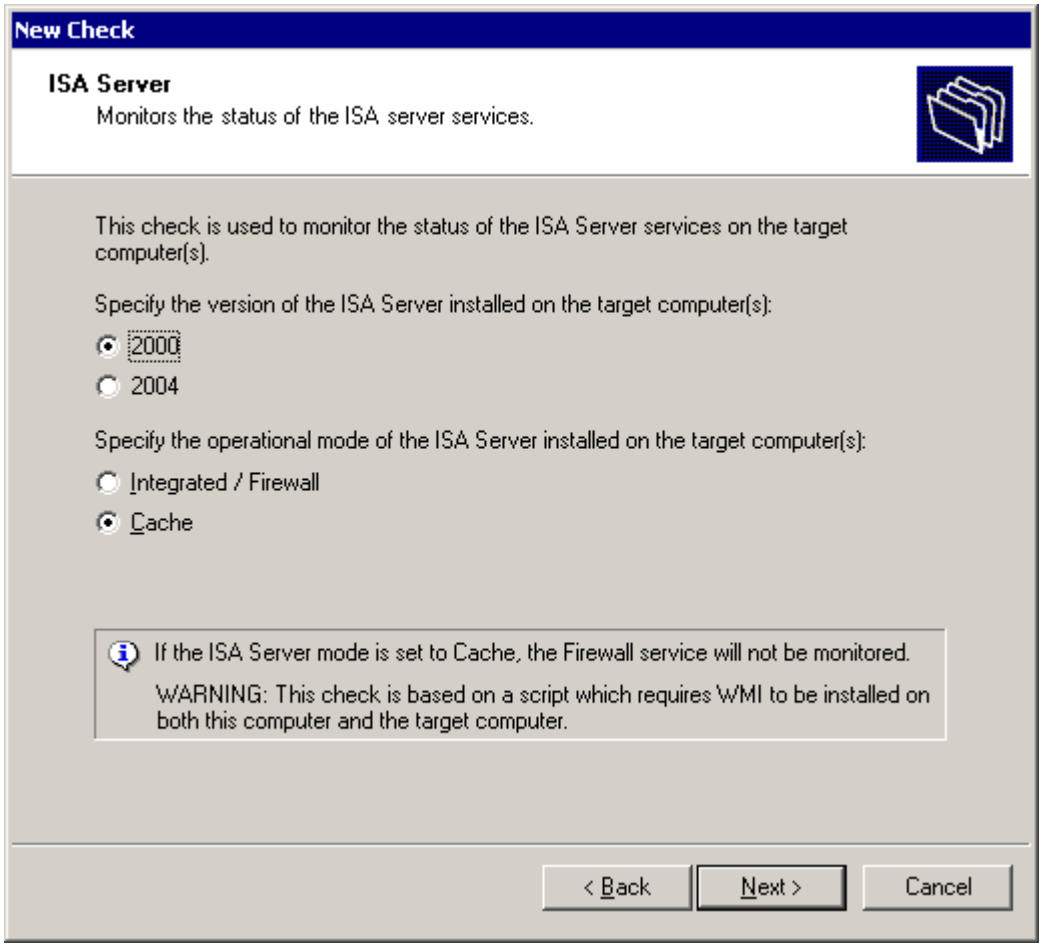
- Domain – Specify the name of the domain in which the group is present (e.g. GFIMALTA).
- Group – Specify the name of the group to be checked (e.g. Domain Admins group)
- Allowed members – Specify the name of the members that are allowed in this group. Separate each member by commas (e.g. JasonM, NickG, AndreM)

4.6 Windows applications checks

4.6.1 Generic ISA Server check

This monitor function requires WMI to be installed on the computer running GFI Network Server Monitor as well as on the computer being monitored. The monitor function will create a VBscript which uses WMI with the parameters you specify in the check parameters dialog. WMI is only available on Windows 2000 and higher computers, therefore this monitor function can only be used if both the GFI Network Server Monitor computer and the computer to be monitored are running Windows 2000 or higher.

GFI Network Server Monitor can monitor the status of ISA Services on target computers.


New Check
ISA Server
Monitors the status of the ISA server services.
This check is used to monitor the status of the ISA Server services on the target computer(s).
Specify the version of the ISA Server installed on the target computer(s):
2000
2004
Specify the operational mode of the ISA Server installed on the target computer(s):
Integrated / Firewall
Cache
If the ISA Server mode is set to Cache, the Firewall service will not be monitored.
WARNING: This check is based on a script which requires WMI to be installed on both this computer and the target computer.
< Back
Next >
Cancel

Screenshot 70 - ISA Server check parameters dialog

The parameters required are:

1. Specify the ISA Server version installed on the target computer.
   - » 2000 – Enable this option, if your target computer has ISA server 2000 installed.
   - » 2004 – Enable this option, if your target computer has ISA server 2004 installed.

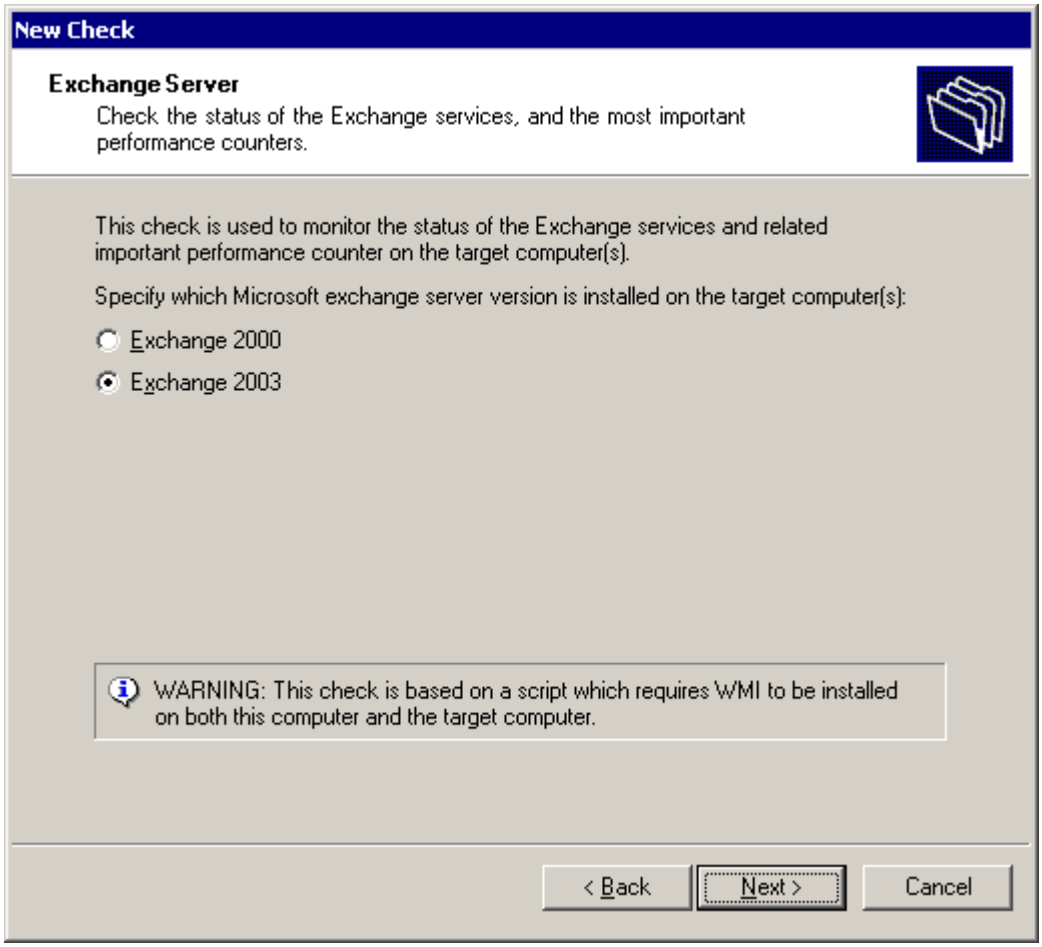
2. Enable '*Integrated / Firewall*' or '*Cache*' option to specify the operation mode of the ISA Server installed on the target computer.

If the ISA Server operation mode is set to Cache, the Firewall services will not be monitored during this check.

4.6.2 Generic Exchange Server check

This monitor function requires WMI to be installed on the computer running GFI Network Server Monitor as well as on the computer being monitored. The monitor function will create a VBscript which uses WMI with the parameters you specify in the check parameters dialog.

GFI Network Server Monitor can monitor the status of Exchange services and performance counters running on a target computer. Supported performance counters include: Information Store performance counters, Mailboxes performance counters, Public folders performance counters, and SMTP service performance counters. Alerts and actions can be triggered whenever the performance of Exchange services runs low.


New Check
Exchange Server
Check the status of the Exchange services, and the most important performance counters.
This check is used to monitor the status of the Exchange services and related important performance counter on the target computer(s).
Specify which Microsoft exchange server version is installed on the target computer(s):
Exchange 2000
Exchange 2003
WARNING: This check is based on a script which requires WMI to be installed on both this computer and the target computer.
< Back
Next >
Cancel

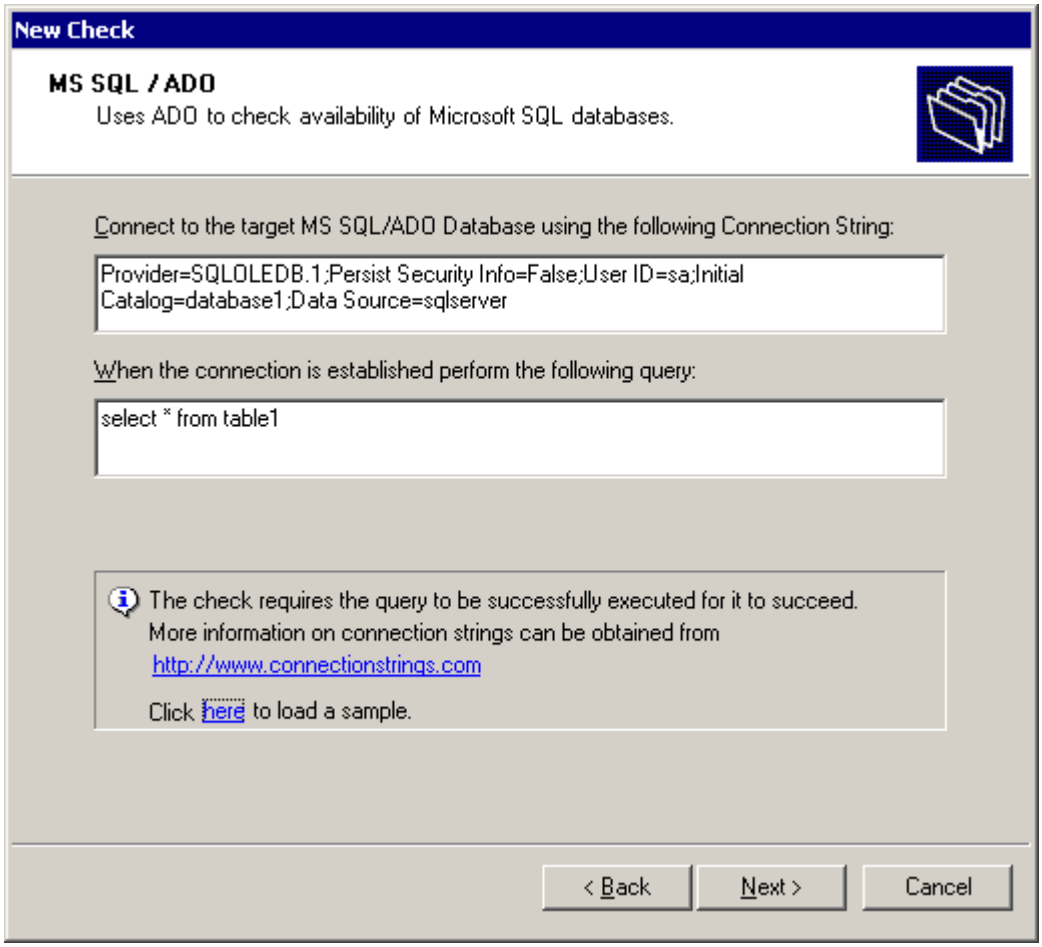
Screenshot 71 - Exchange server check parameters dialog

The Exchange server check requires the following parameters:

1. Specify the MS Exchange Server version installed on the target computer(s):
   - » Exchange 2000 – Enable this option if the target computer is running Exchange server 2000.
   - » Exchange 2003 – Enable this option if the target computer is running Exchange server 2003.

4.6.3 Generic MS SQL/ADO check

GFI Network Server Monitor uses ADO (ActiveX Data Object) to check for the availability of Microsoft SQL databases. It provides a DSN-less connection to a variety of databases, like MS SQL and MS Access.


New Check
MS SQL / ADO
Uses ADO to check availability of Microsoft SQL databases.
Connect to the target MS SQL/ADO Database using the following Connection String:
Provider=SQLOLEDB.1;Persist Security Info=False;User ID=sa;Initial Catalog=database1;Data Source=sqlserver
When the connection is established perform the following query:
select * from table1
The check requires the query to be successfully executed for it to succeed.
More information on connection strings can be obtained from
http://www.connectionstrings.com
Click here to load a sample.
< Back
Next >
Cancel

Screenshot 72 - MS SQL/ADO check parameters dialog

An MS SQL / ADO function requires the following parameters:

- ADO Connection String – Specify the ADO connection string which will be used to connect to the SQL Server/Data source.
- Query – Specify the SQL Query which will be triggered when connection is established.

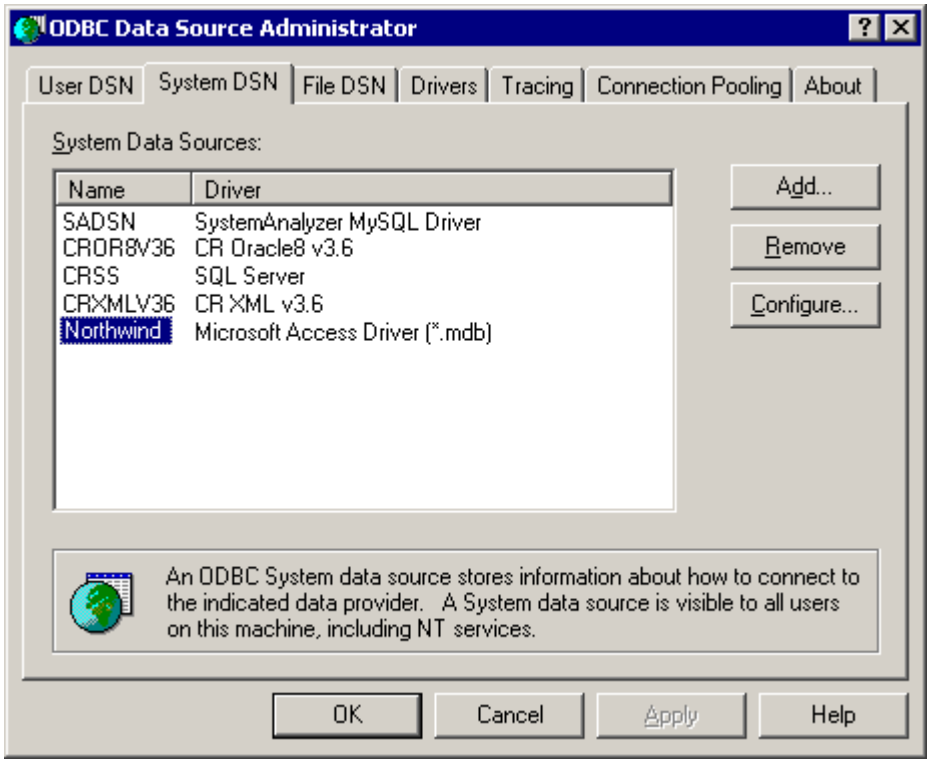
For more information on SQL/ADO connections strings, please visit http://www.connectionstrings.com

4.7 Windows OS databases checks

4.7.1 Generic - ODBC

GFI Network Server Monitor makes use of ODBC to check for the availability of a variety of databases. Major database systems that support ODBC include: Microsoft SQL Server, Microsoft Access, Microsoft Excel, Oracle, FoxPro, Paradox, SyBase, Informix, OpenIngres, InterBase, Progress, IBM LANDP, DB2 and AS/400.

To monitor a database via ODBC, you must first setup a System DSN entry to the database you wish to monitor on the server running GFI Network Server Monitor.



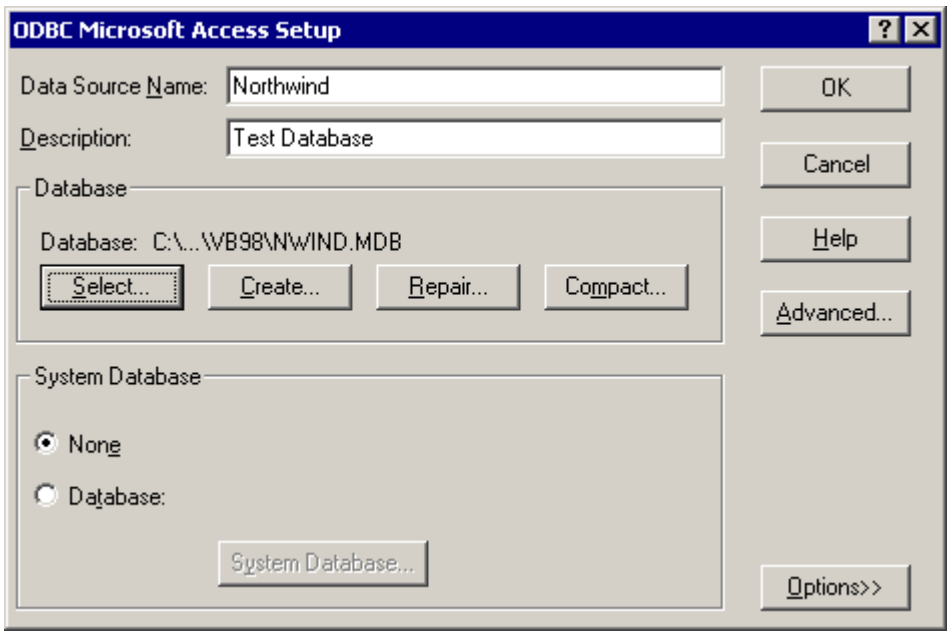
Screenshot 73 - ODBC administrator with sample database configured

A system DSN entry is setup as follows

1. Go to Administrative tools > Data Sources (ODBC) to launch the ODBC administrator.

2. Click on the 'System DSN' tab then click on 'Add'.

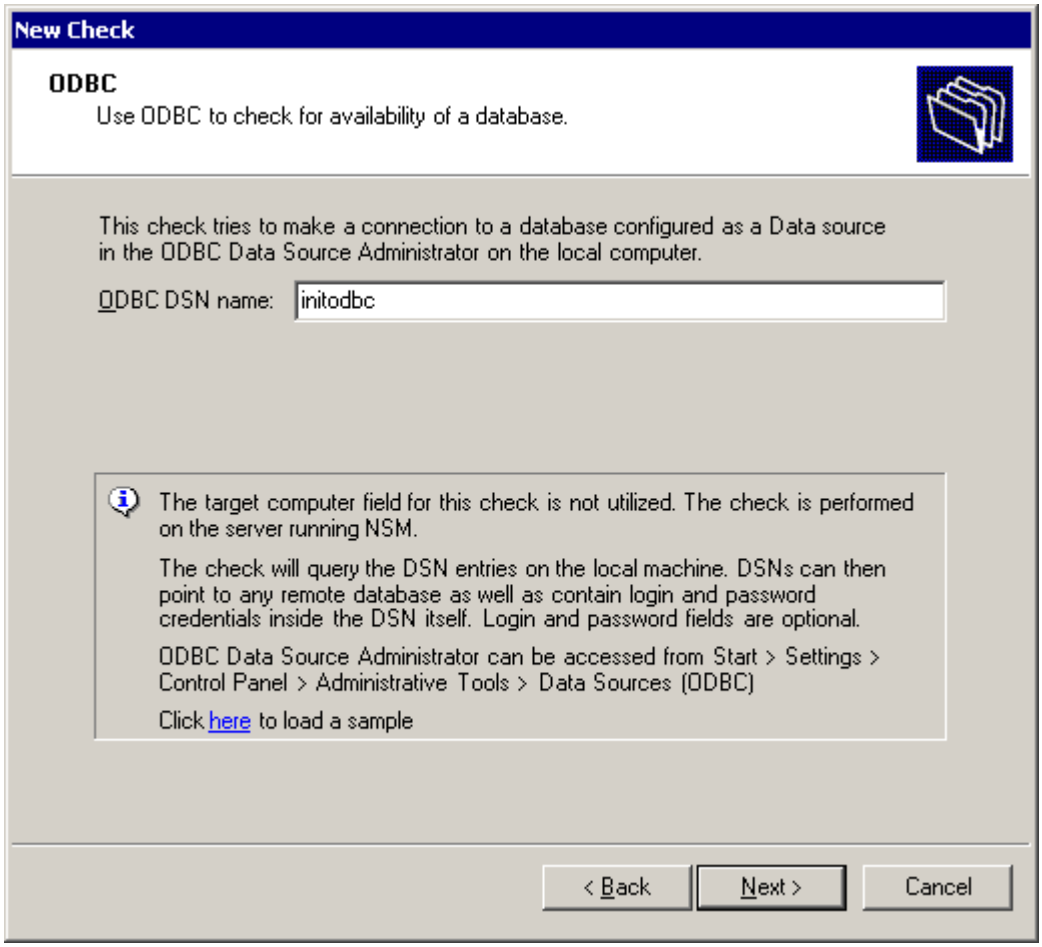
It is important that you select 'System DSN' and not 'User DSN' otherwise the service will not have access to the data source/database.



Screenshot 74 - ODBC setup with sample database

3. Select a database driver suitable for the database you wish to monitor (e.g. for an MS Access database choose Microsoft Access Driver (*.mdb)).

4. In the ODBC setup dialog, specify a data source name (e.g. MY_Dbase) and select the database you wish to monitor. In this example we have used the 'Northwind' database. Click on 'OK' to add the data source.


New Check
ODBC
Use ODBC to check for availability of a database.
This check tries to make a connection to a database configured as a Data source in the ODBC Data Source Administrator on the local computer.
ODBC DSN name:
initodbc
The target computer field for this check is not utilized. The check is performed on the server running NSM.
The check will query the DSN entries on the local machine. DSNs can then point to any remote database as well as contain login and password credentials inside the DSN itself. Login and password fields are optional.
ODBC Data Source Administrator can be accessed from Start > Settings > Control Panel > Administrative Tools > Data Sources (ODBC)
Click here to load a sample
< Back
Next >
Cancel

Screenshot 75 - Generic ODBC properties

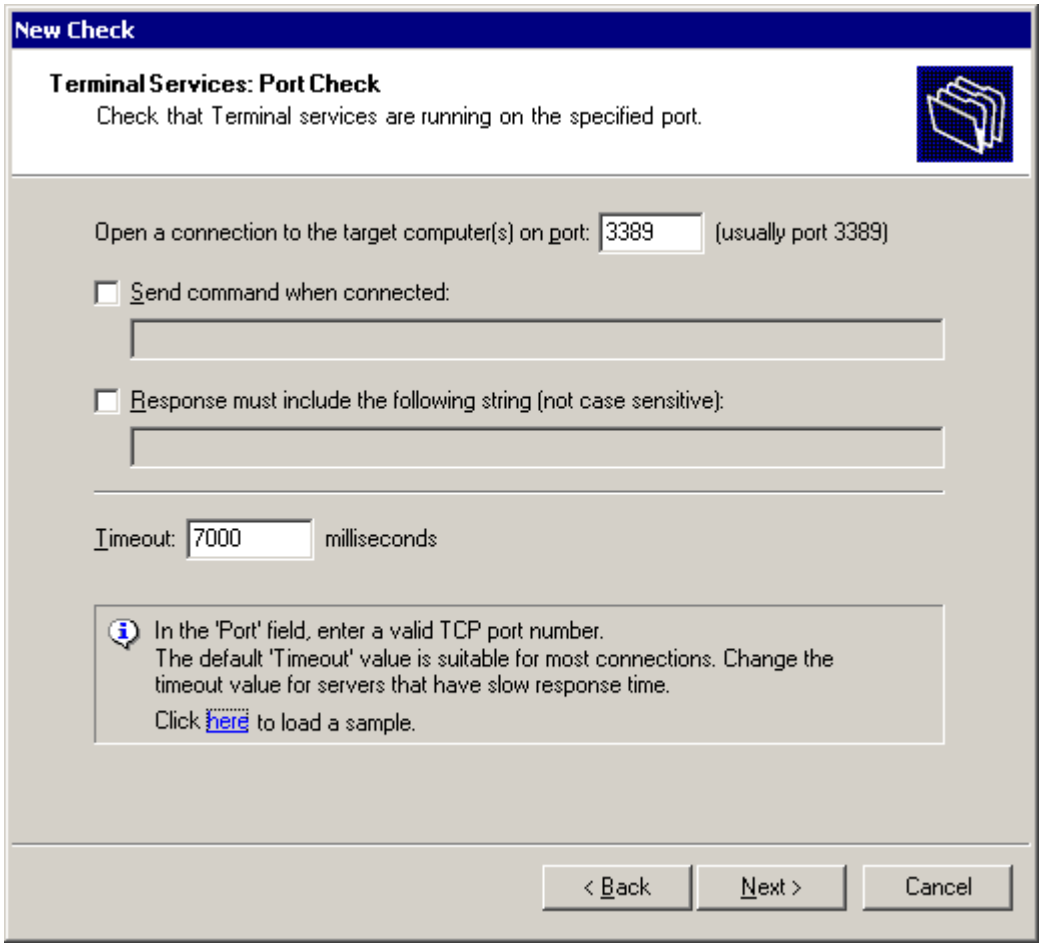
The ODBC check requires the following parameter:

» *ODBC DSN name* - Specify the ODBC data source name (e.g. Northwind).

4.8 Terminal Services checks

4.8.1 Terminal Services Port Check

GFI Network Server Monitor can check if Local or Remote servers have their terminal services port enabled. This is done by establishing a handshake connection on the remote TCP port (by default port 3389) of the target computer.


New Check
Terminal Services: Port Check
Check that Terminal services are running on the specified port.
Open a connection to the target computer(s) on port: 3389 (usually port 3389)
Send command when connected:
Response must include the following string (not case sensitive):
Timeout: 7000 milliseconds
In the 'Port' field, enter a valid TCP port number.
The default 'Timeout' value is suitable for most connections. Change the timeout value for servers that have slow response time.
Click here to load a sample.
< Back
Next >
Cancel

Screenshot 76 - Terminal Services: Port Check parameters dialog

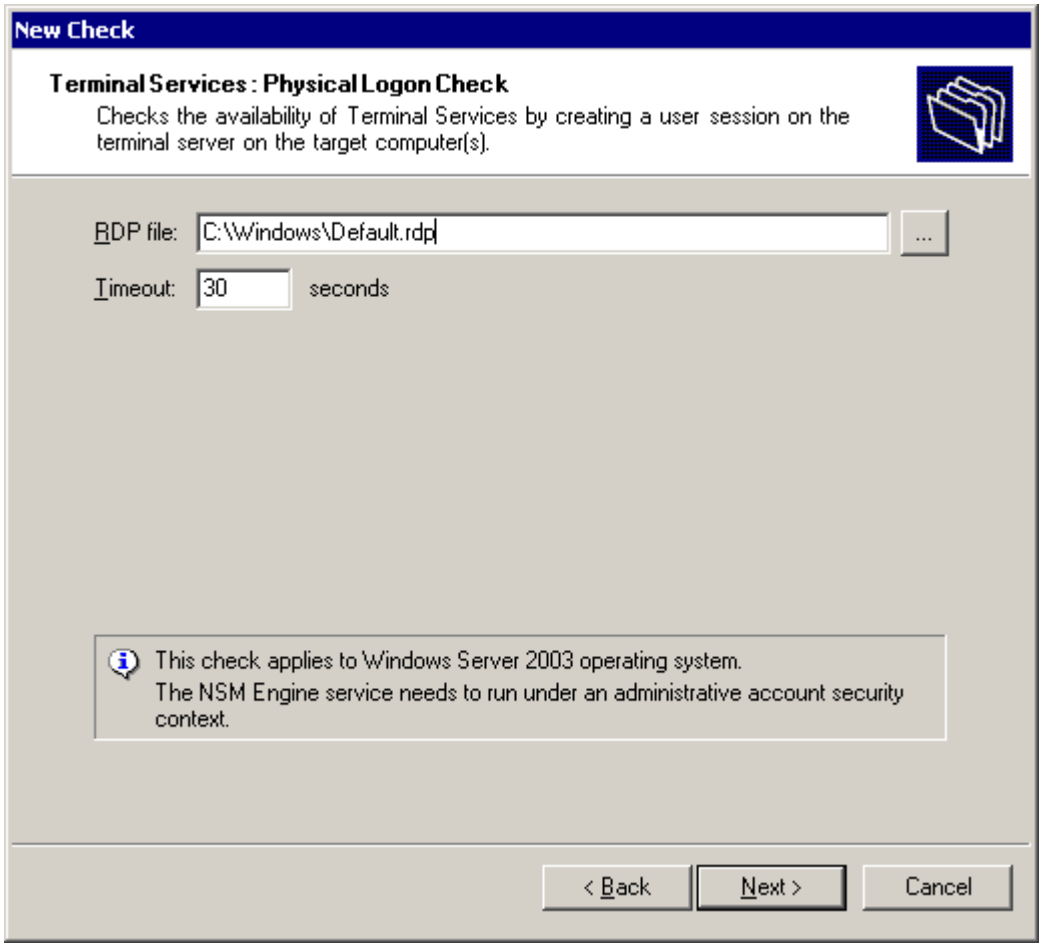
A Terminal Services check requires the following parameters:

- Port – Specify the TCP port number which will be used for communicating with a target computer. The default TCP port is 3389.
- Send command when connected – Enable this option to send the specified command as soon as connection is established.
- Response must include the following string – Enable this option and specify the string which must be present in the response. The default response for SMTP servers generally includes: '200'.
- Timeout – Specify the number of milliseconds before the function times out. Usually, a connection to the server is established within 1 second. However, some slow/busy servers need more time. Recommended value is 7000 milliseconds.

Terminal Services checks must run under a Local or Domain Administrative account. Failure to run this check under such security contexts will cause this check to fail with the error: "Failed to establish a terminal server connection".

4.8.2 Terminal Services Physical Logon Check

GFI Network Server Monitor can check for the availability of Terminal Services by simulating a remote user session on the terminal server of the target computer.


New Check
Terminal Services : Physical Logon Check
Checks the availability of Terminal Services by creating a user session on the terminal server on the target computer(s).
RDP file:
C:\Windows\Default.rdp
...
Timeout:
30
seconds
This check applies to Windows Server 2003 operating system.
The NSM Engine service needs to run under an administrative account security context.
< Back
Next >
Cancel

Screenshot 77 - Terminal Services: Physical Logon check parameters dialog

The parameters required by this function are:

- RDP File – Specify path were the Remote Desktop Protocol (RDP) file is located (e.g. C:\Documents and Settings\<relative user folder>\Recent\default.rdp).
- Timeout – Specify the number of milliseconds before the function times out. Usually, a connection to the server is established within 1 second. However, some slow/busy servers need more time. Recommended value is 7000 milliseconds.

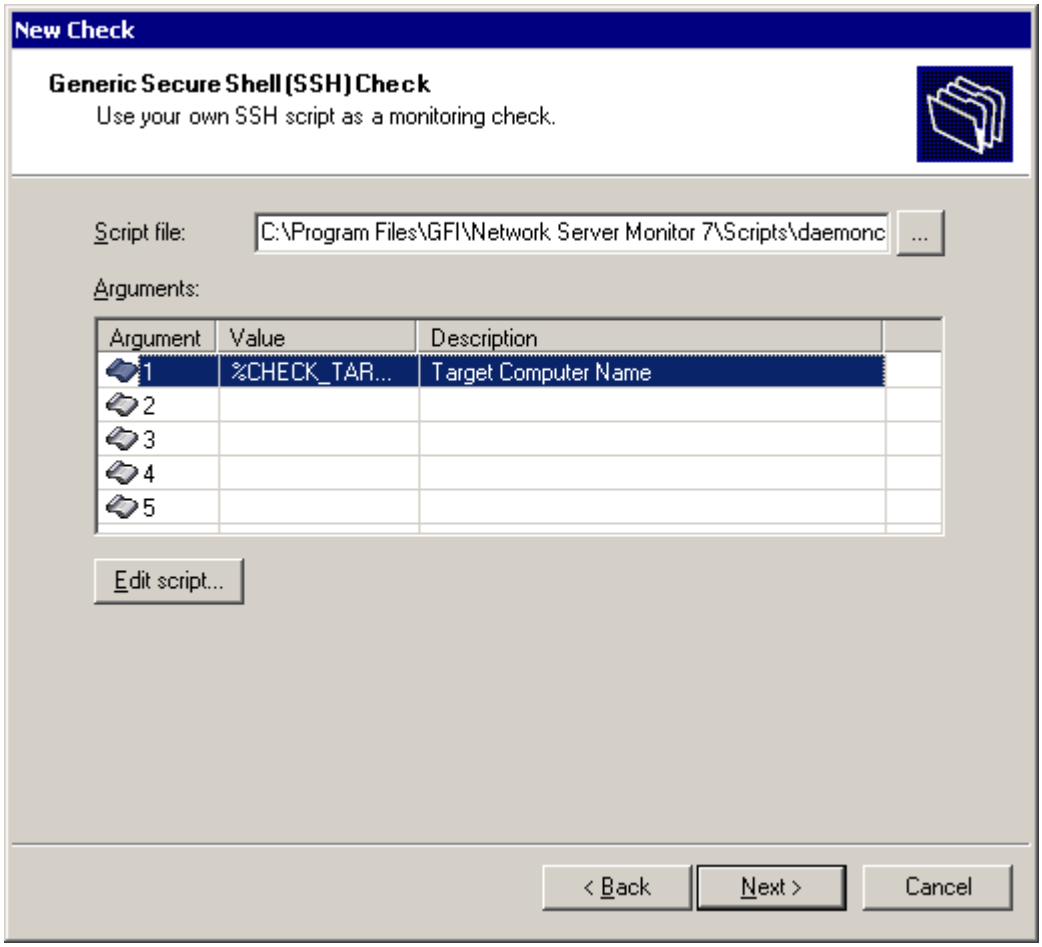
The RDP file is generated by the Remote Desktop connection client whenever a remote session is established (e.g., Default.rdp). This file contains properties and parameters relative to the remote connection session made, including authentication details and display settings which are used during each remote session.

Terminal Services checks must run under a Local or Domain Administrative account. Otherwise, these checks will fail with error: "Failed to establish a terminal server connection".

4.9 Linux / Unix OS generic checks

4.9.1 Generic Secure Shell (SSH) Check

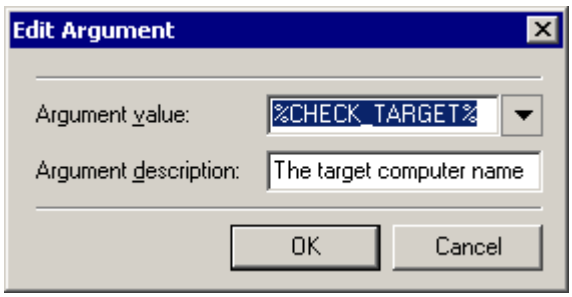
The SSH Check function allows you to create custom monitor functions which can be remotely executed on Unix/Linux based computers through the Secure Shell (SSH) service running on that computer. Secure Shell, sometimes known as Secure Socket Shell, is a Unix-based command interface and protocol for securely getting access to a remote computer.



Screenshot 78 - SSH check parameters dialog

A Generic SSH Script Check requires the following parameters:

» *Script file* – Specify the path to the SSH script file which will be used by the monitoring check to test the specified target computer(s).



Screenshot 79 - The parameters dialog

» *Arguments* – In the arguments list, specify any additional parameters required by this function. During check execution these parameters will be automatically passed on to the SSH script in the order specified in the arguments list. To add a parameter, double click on the position/row where you wish to add an additional argument and specify the required values in the parameters dialog. Parameter values can be specified as a string or can be passed on through system variables (e.g. %USERNAME%).

Strings which contain spaces must be specified within double quotes (“”) e.g. “Mail Server”.

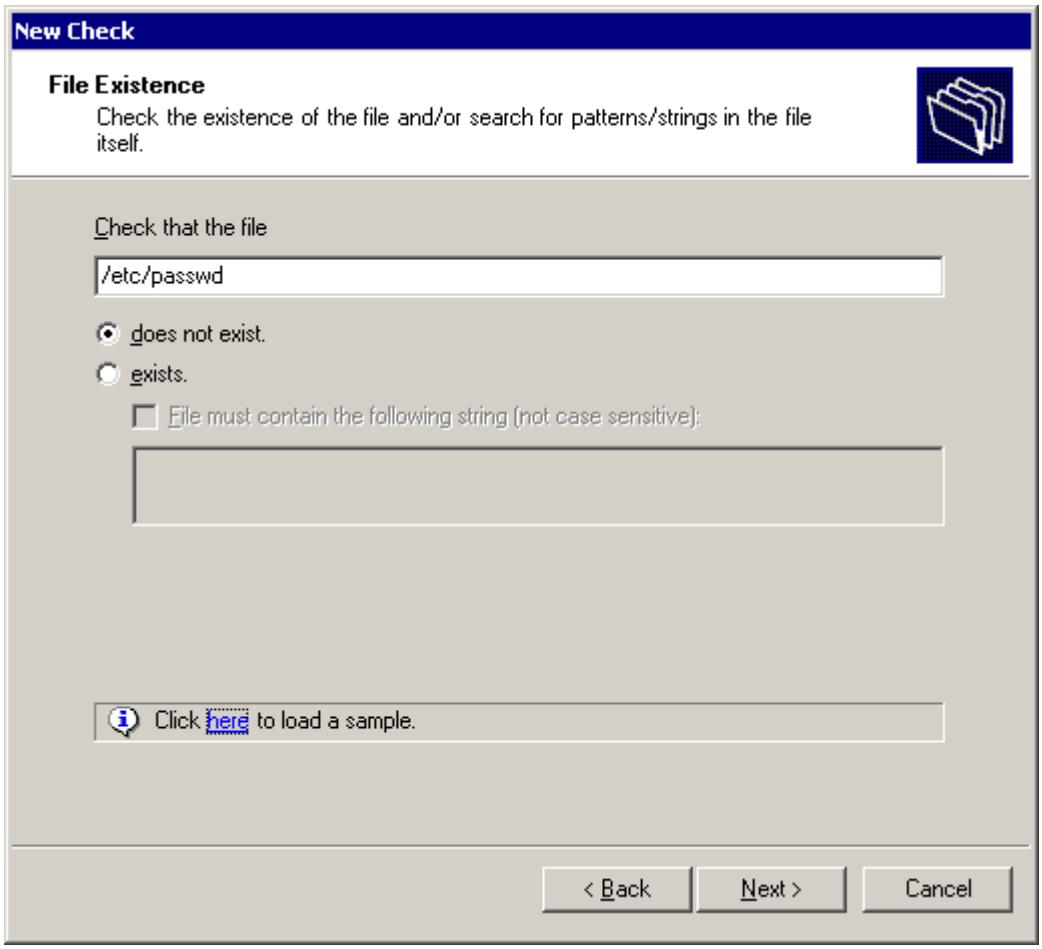
You can make changes to the selected script file by clicking on the ‘Edit script …’ button.

The “Generic Secure Shell (SSH) Check” requires logon credentials (i.e. username and password or Private Key file) to connect (authenticate) and run SSH scripts on a remote Unix-based target computer. These credentials must be specified from the ‘Logon Credentials’ tab available in the properties of the relative check. For more information on logon credentials, please refer to the ‘Logon credentials’ section in the ‘Configuring GFI Network Server Monitor’ chapter.

4.10 Linux/Unix Operating System Checks

4.10.1 File existence Check

GFI Network Server Monitor can search for specific files in a target computer running on Linux or Unix (e.g. you can use this check to look for scheduled batch job results. If the file exists, you will receive a confirmation stating that the scheduled batch jobs have been executed). You can also search the contents of an existing file for a specified string (e.g. searching for “fail” or “failed” strings in the results file of scheduled batch jobs can help you define if all jobs were successful).


New Check
File Existence
Check the existence of the file and/or search for patterns/strings in the file itself.
Check that the file
/etc/passwd
does not exist.
exists.
File must contain the following string (not case sensitive):
Click here to load a sample.
< Back
Next >
Cancel

Screenshot 80 - File Existence check parameters dialog

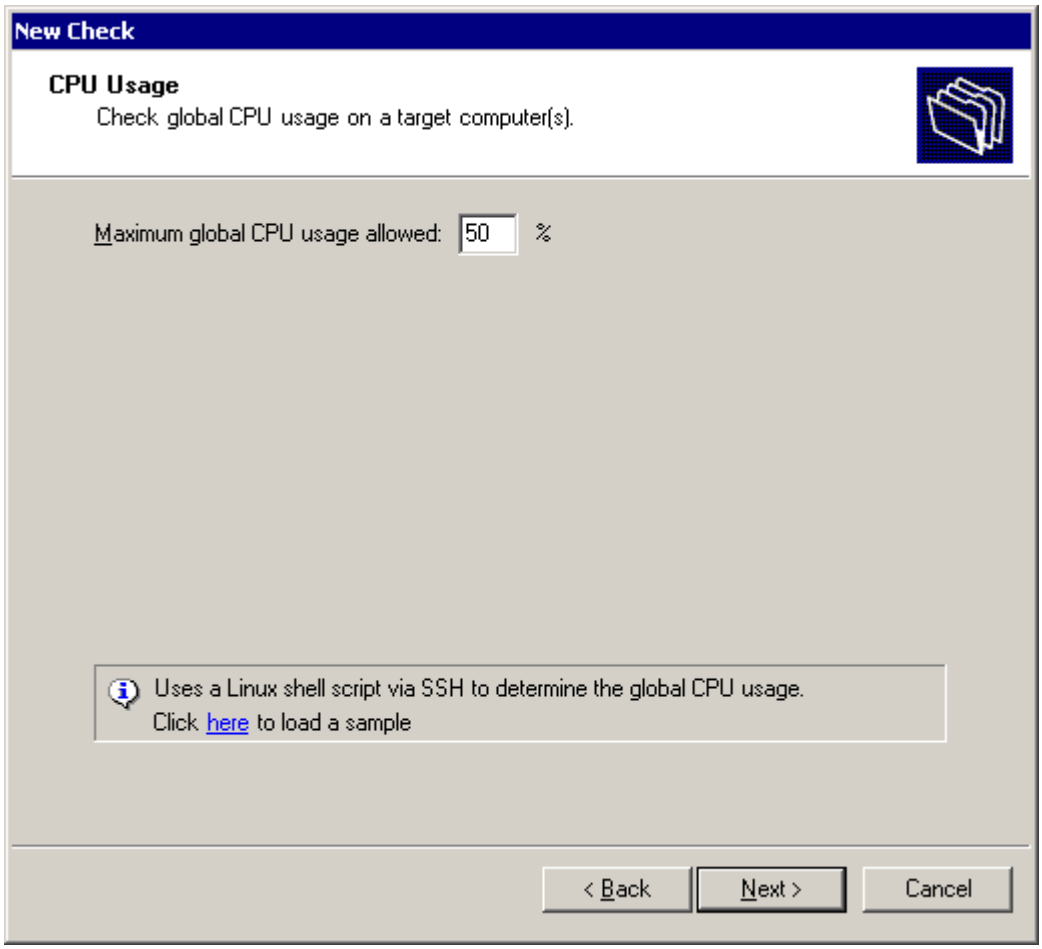
A File Existence function requires the following parameters:

- File (UNC Path) – Specify the complete path to the file (e.g. /etc/password).
- Does not exist – Enable this option to check for file existence only. In this case, the check fails if the specified file is found.
- Exists - Enable this option to check for file existence only. In this case, the check succeeds if the specified file is found.

- File must contain …string – Enable this flag and specify the string to be searched for in the existing file contents. In this case the check will succeed only if the file exists and the specified string is present in the file contents.

4.10.2 CPU usage Check

GFI Network Server Monitor can monitor the CPU usage of a target computer running on Linux / Unix. This function uses a Linux shell script to determine, via SSH, the global CPU usage and can send alerts or trigger actions when the processor usage exceeds the specified CPU usage limit.


New Check
CPU Usage
Check global CPU usage on a target computer(s).
Maximum global CPU usage allowed:
50
%
Uses a Linux shell script via SSH to determine the global CPU usage.
Click here to load a sample
< Back
Next >
Cancel

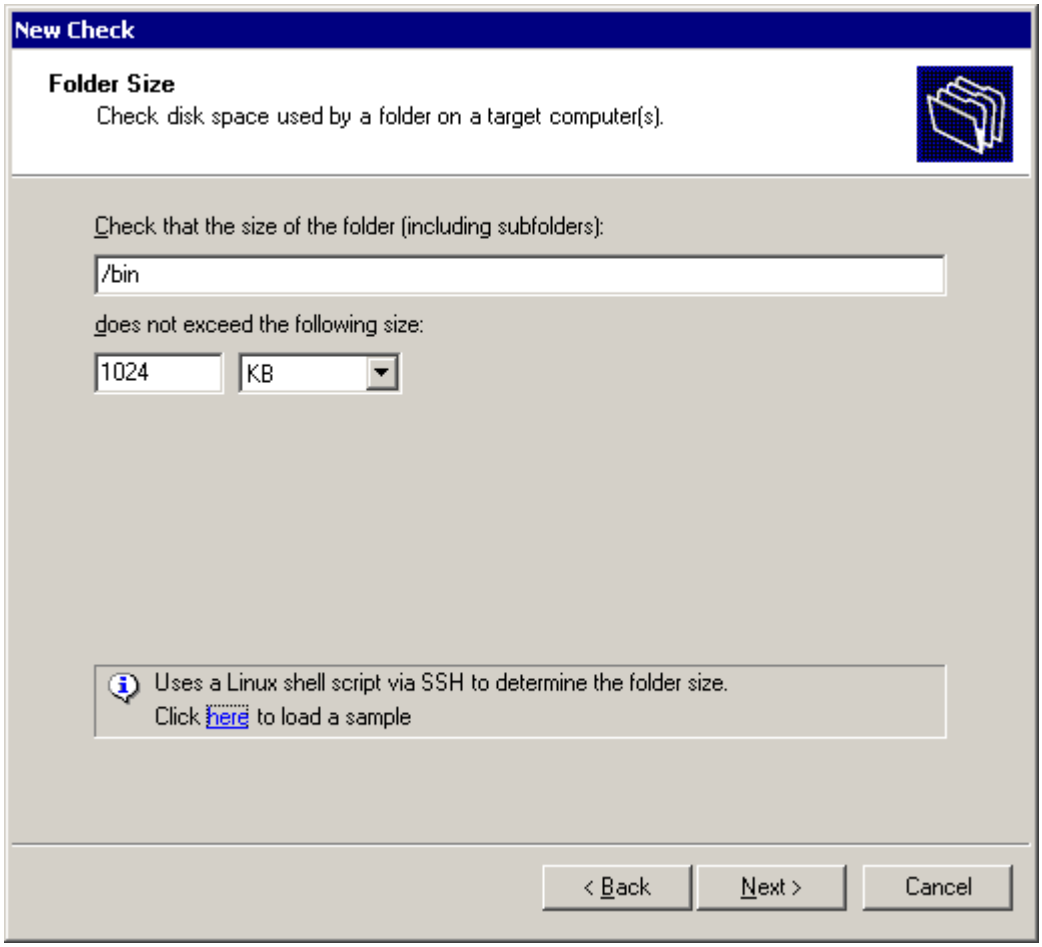
Screenshot 81 - CPU usage setup window

A CPU Usage function takes the following parameter:

- *Maximum global CPU usage allowed* – Specify the maximum % CPU usage allowed on the target computer being monitored.

4.10.3 Directory size Check

GFI Network Server Monitor can check the size of directories located on target computers running on Linux/Unix. You can use this function as a disk quota manager which can send alerts when a directory exceeds the specified size.


New Check
Folder Size
Check disk space used by a folder on a target computer(s).
Check that the size of the folder (including subfolders):
/bin
does not exceed the following size:
1024
KB
Uses a Linux shell script via SSH to determine the folder size.
Click here to load a sample
< Back
Next >
Cancel

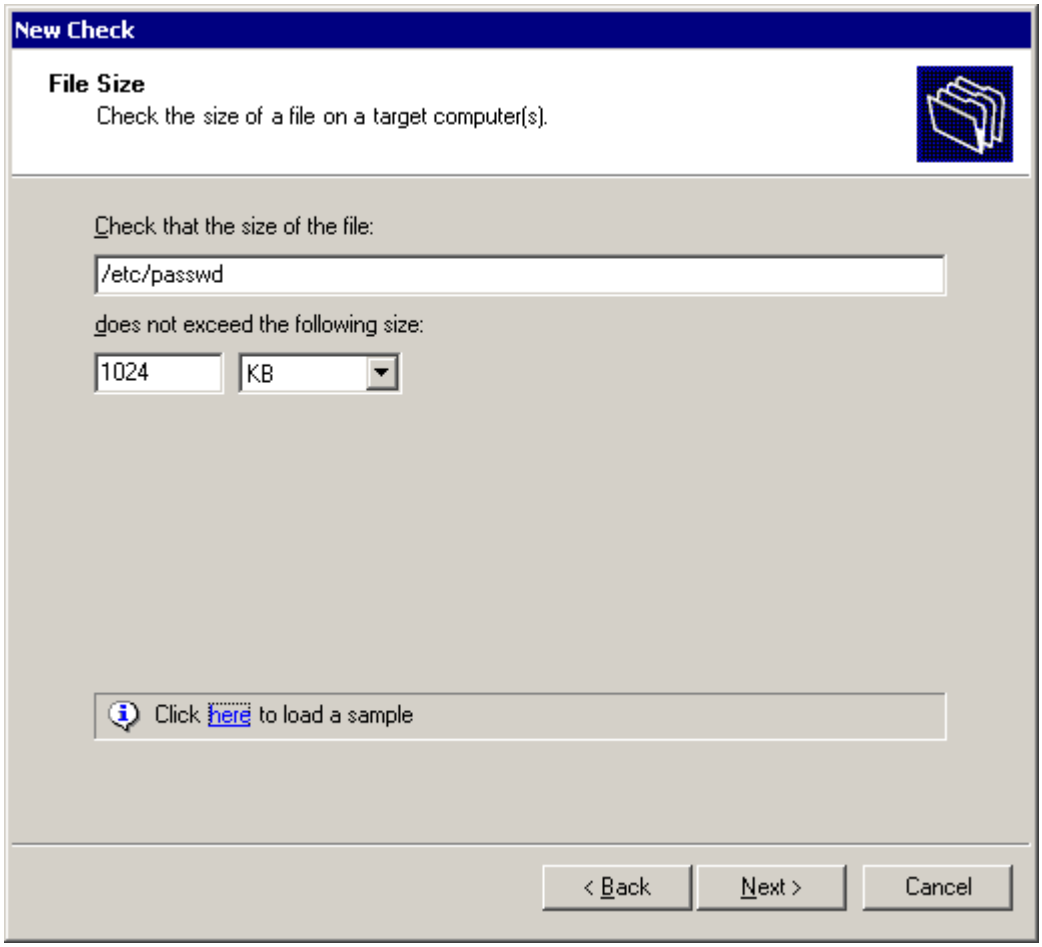
Screenshot 82 - Directory/folder Size setup window

A Directory Size function requires the following parameters:

- Directory Name – Specify the path to the directory to be monitored (e.g. /user/personal).
- Directory size – Specify the maximum size (in KB, MB or GB) allowed for this directory.

4.10.4 File size Check

GFI Network Server Monitor can check the size of files on target computers running on Linux/Unix. This function can be used as a disk quota manager which can send alerts when a specific file exceeds the specified size (e.g. you can receive alerts when the system status log file exceeds the specified size, enabling you to free used disk space).



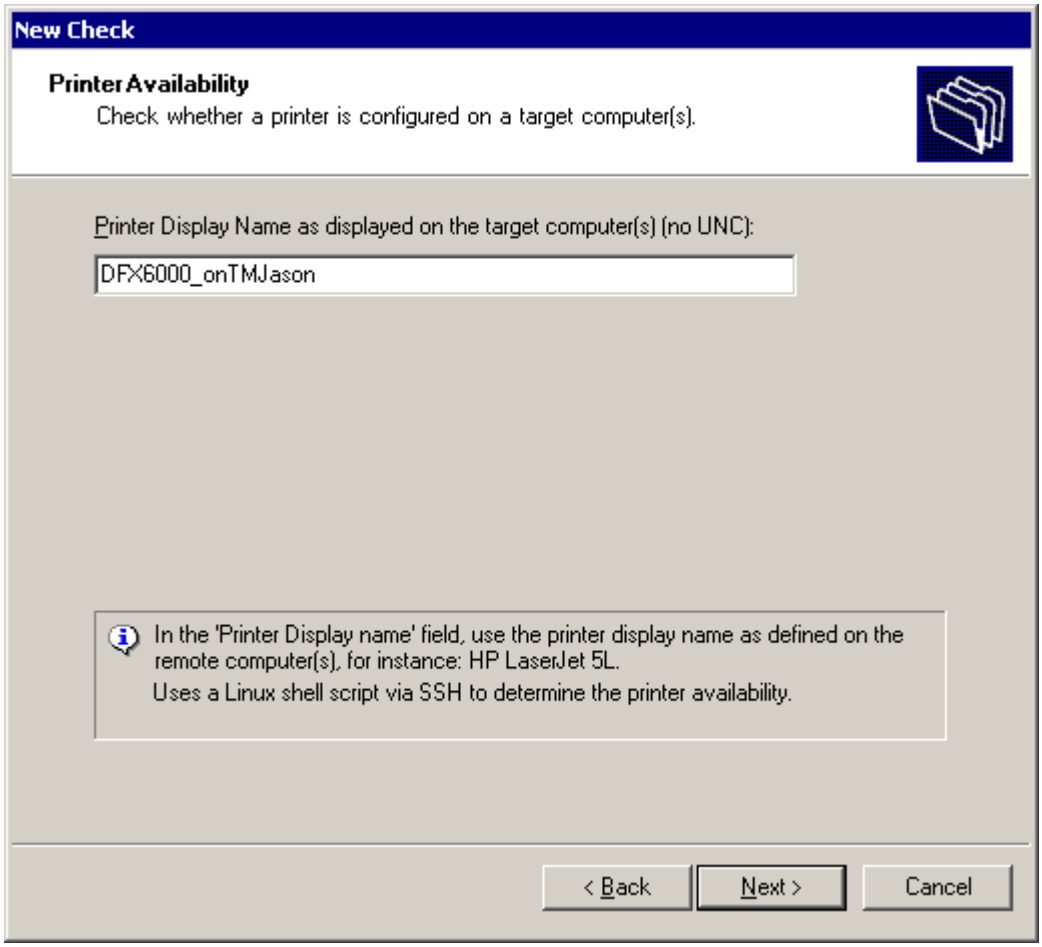
Screenshot 83 - File size check parameters dialog

The File Size function requires the following parameters:

- File name – Specify the complete path to the file which needs to be monitored (e.g. /data/sys_log).
- File size limit – Specify the maximum size (in KB, MB or GB) allowed for this file.

4.10.5 Printer availability Check

GFI Network Server Monitor can check for the availability of network printers connected to target computers running on Linux / Unix. When a printer problem occurs, alerts can be sent to the support personnel in order for them to take immediate action and get the printer back online or transfer print jobs to a different printer.


New Check
Printer Availability
Check whether a printer is configured on a target computer(s).
Printer Display Name as displayed on the target computer(s) (no UNC):
DFX6000_onTMJason
In the 'Printer Display name' field, use the printer display name as defined on the remote computer(s), for instance: HP LaserJet 5L.
Uses a Linux shell script via SSH to determine the printer availability.
< Back
Next >
Cancel

Screenshot 84 - Printer check parameters dialog

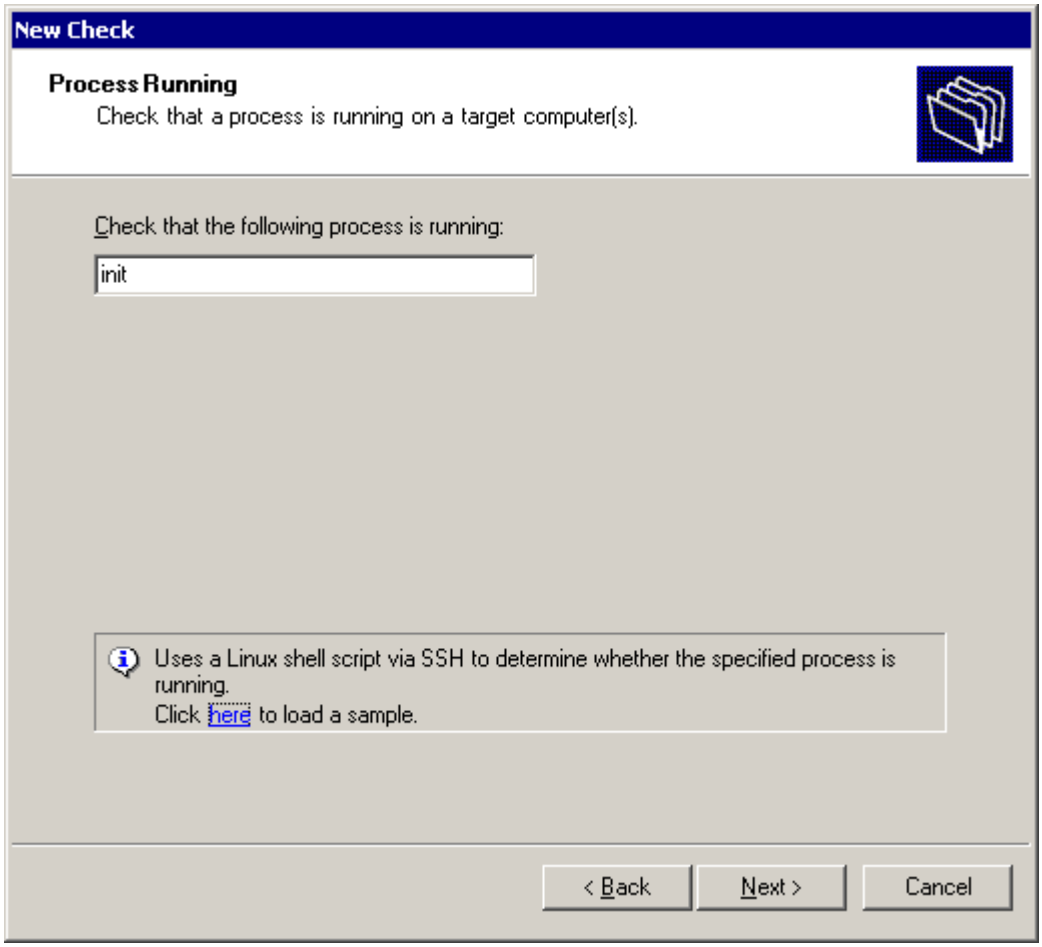
GFI Network Server Monitor uses a Linux shell script, via SSH, to determine printer availability.

A Printer Availability check requires the following parameters:

- *Printer name* – Specify the name of the printer to be monitored.

4.10.6 Process Running Check

GFI Network Server Monitor enables you to check processes on local and remote target computers running on Linux/Unix. If a process is active, then the target computer is considered to be available.


New Check
Process Running
Check that a process is running on a target computer(s).
Check that the following process is running:
init
Uses a Linux shell script via SSH to determine whether the specified process is running.
Click here to load a sample.
< Back
Next >
Cancel

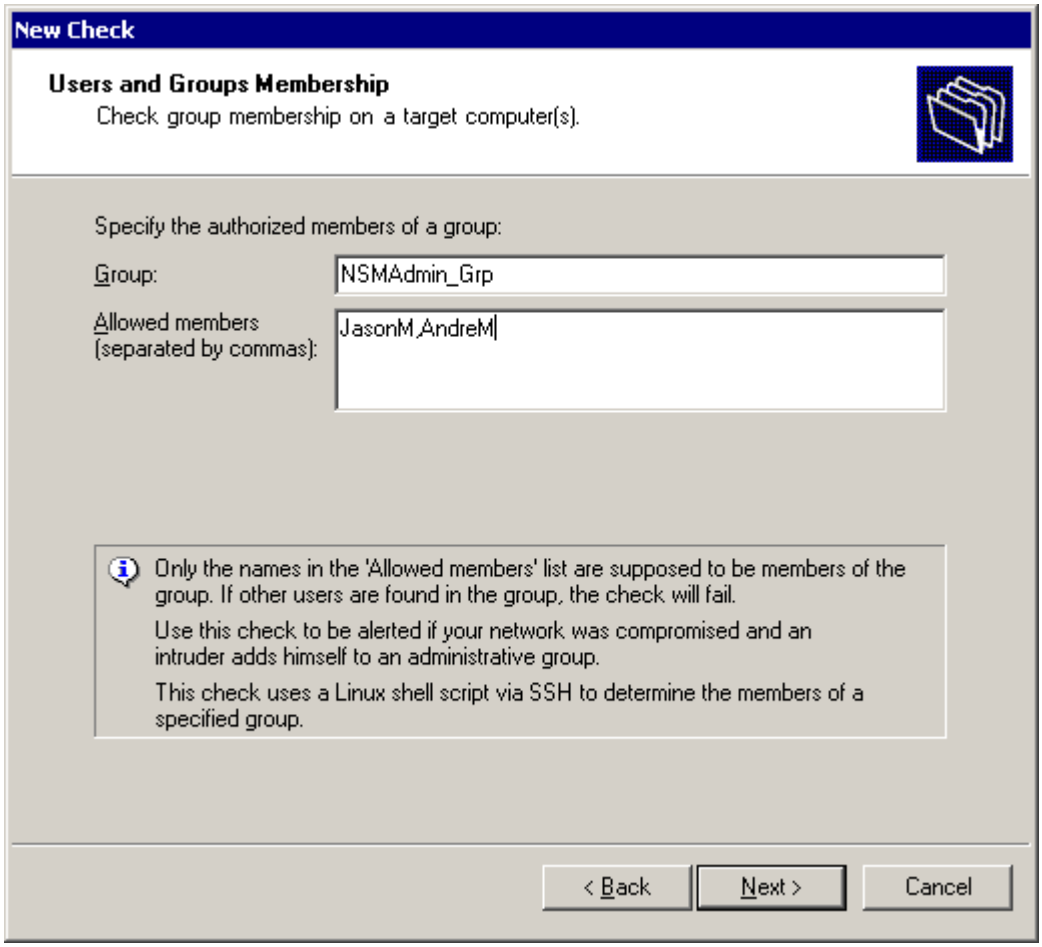
Screenshot 85 -Running Process check parameters dialog

A process check requires the following parameter:

- Process – Specify the name of the process to be monitored (e.g. init).

4.10.7 Users and groups membership Check

GFI Network Server Monitor inspects groups and group membership against intruders which could pose a vulnerability threat to your network system (e.g. Intruders in Domain Administrators group can give themselves administrative rights).


New Check
Users and Groups Membership
Check group membership on a target computer(s).
Specify the authorized members of a group:
Group:
NSMAdmin_Grp
Allowed members (separated by commas):
JasonM,AndreM
Only the names in the 'Allowed members' list are supposed to be members of the group. If other users are found in the group, the check will fail.
Use this check to be alerted if your network was compromised and an intruder adds himself to an administrative group.
This check uses a Linux shell script via SSH to determine the members of a specified group.
< Back
Next >
Cancel

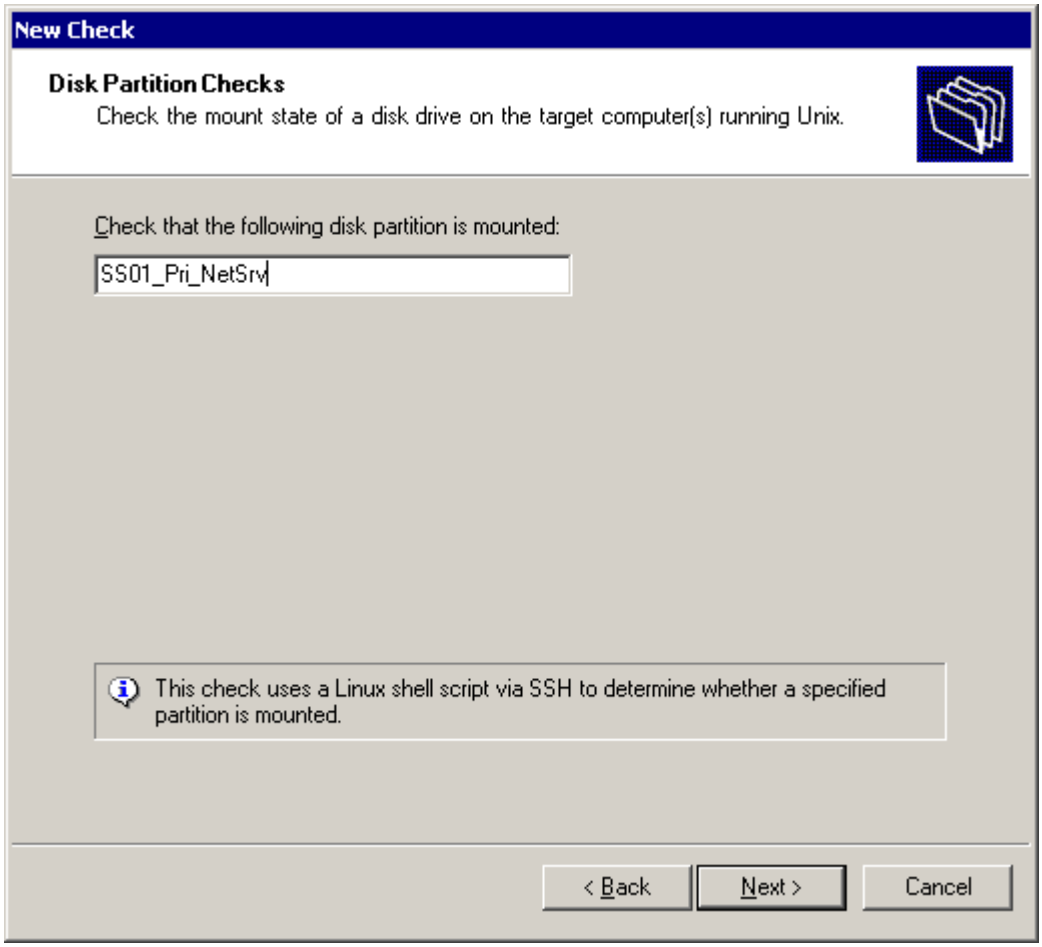
Screenshot 86 - Users and Groups check parameters dialog

The User/Group membership function requires the following parameters:

- Group – Specify the name of the group to be checked against intruders.
- Allowed members – Specify the list of authorized members in the specified group. Separate each member by a comma (e.g. JasonM, NickG, AndreM).

4.10.8 Disk Partition Checks

GFI Network Server Monitor uses a Linux Shell script to check the state of mounted disk drives on a target computer running on Linux/Unix.


New Check
Disk Partition Checks
Check the mount state of a disk drive on the target computer(s) running Unix.
Check that the following disk partition is mounted:
SS01_Pri_NetSrv
This check uses a Linux shell script via SSH to determine whether a specified partition is mounted.
< Back
Next >
Cancel

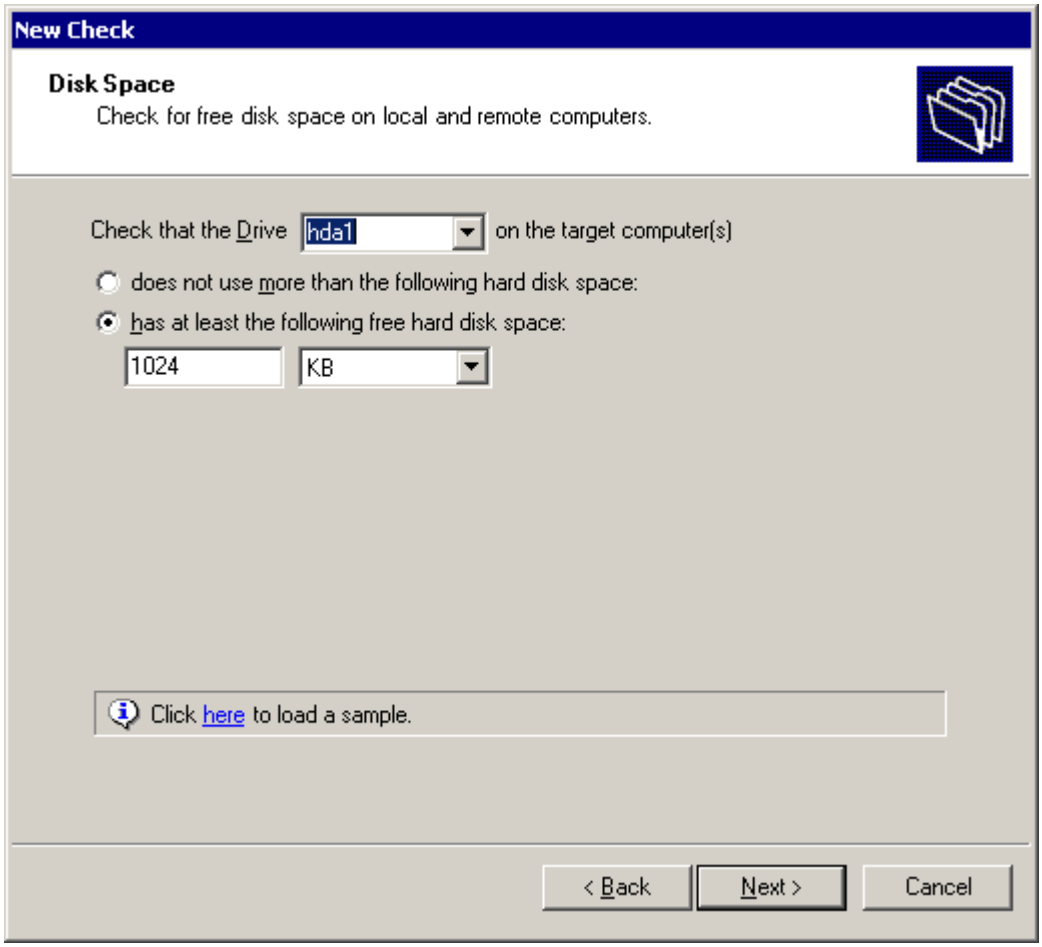
Screenshot 87 - Disk Partition check parameters dialog

The parameters required by this function are:-

» *Partition label* – Specify the identification name of the disk partition to be checked.

4.10.9 Disk Space Check

GFI Network Server Monitor can check for available free or used disk space information on local and remote target computers running on Linux/Unix. Alerts can be sent when the used or free space exceeds a specified limit.


New Check
Disk Space
Check for free disk space on local and remote computers.
Check that the Drive
hda1
on the target computer(s)
does not use more than the following hard disk space:
has at least the following free hard disk space:
1024
KB
Click here to load a sample.
< Back
Next >
Cancel

Screenshot 88 - Disk Space check parameters dialog.

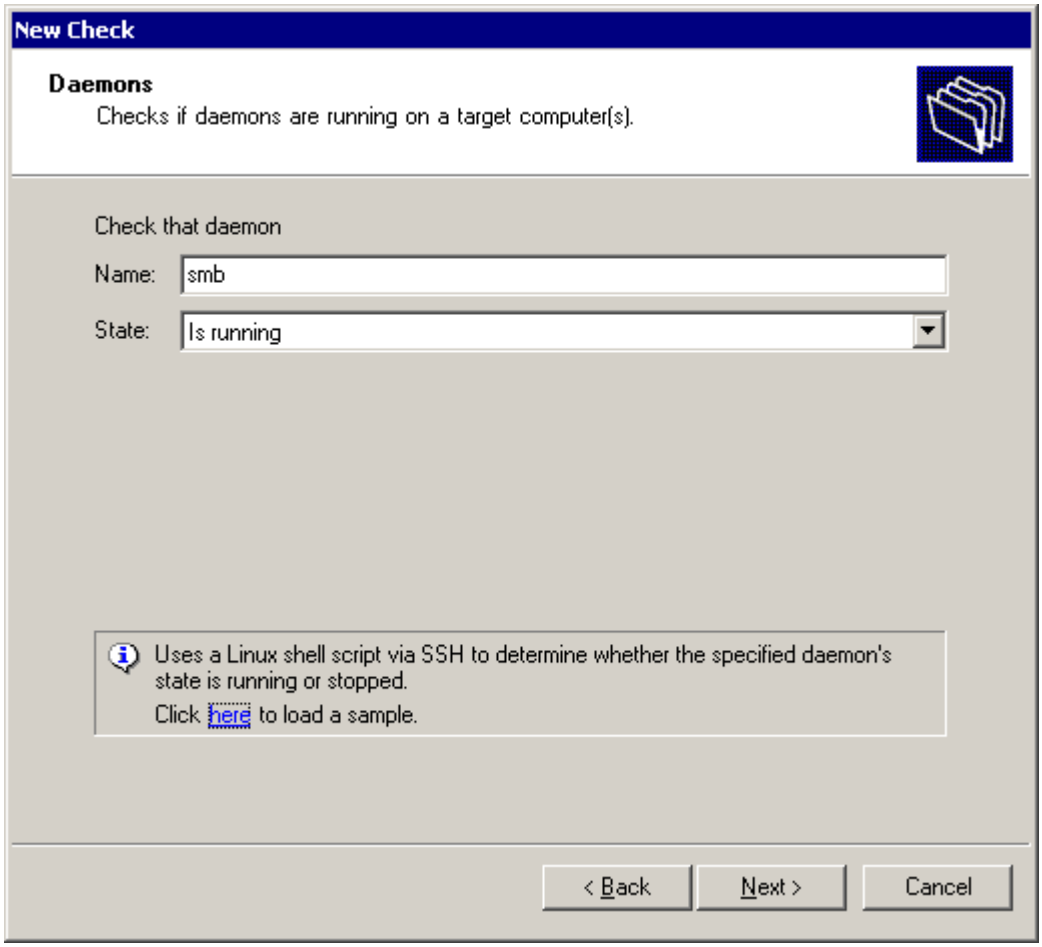
A Disk Space function requires the following parameters:

- Check that the Drive – Specify the drive to be checked.
- Does not use more than the following hard disk space – Enable this option and specify the maximum disk space (in KB, MB or GB) allowed for use on this particular drive, i.e. the check will fail if the used disk space exceeds the specified value.
- Has at least the following free hard disk space – Enable this option and specify the minimum free space value allowed on this particular drive, i.e. the check will fail if free disk space is less than the specified amount.

4.10.10 Daemon check

GFI Network Server Monitor can check if a target daemon is running on a target Linux/Unix computer. Daemons are background programs that run without human intervention to accomplish a specific task (usually providing a service).

The daemon check uses Secure Shell (SSH) to remotely execute a Linux Shell script which determines the state (i.e., running or stopped) of a specific daemon.


New Check
Daemons
Checks if daemons are running on a target computer(s).
Check that daemon
Name:
smb
State:
Is running
Uses a Linux shell script via SSH to determine whether the specified daemon's state is running or stopped.
Click here to load a sample.
< Back
Next >
Cancel

Screenshot 89 - Daemon check properties dialog

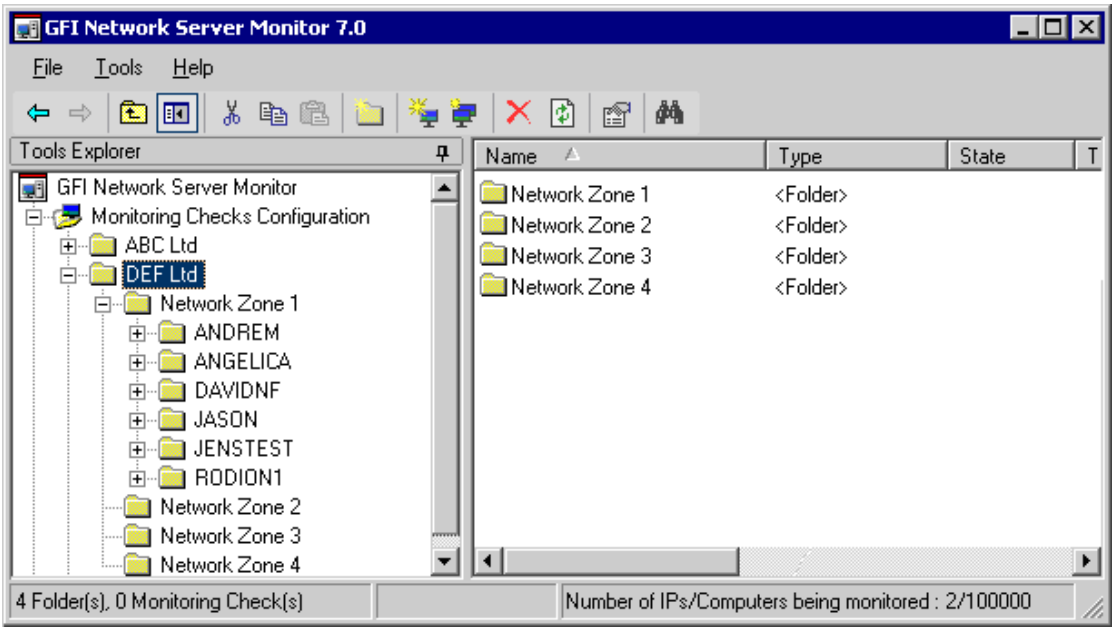
The Daemons check requires the following parameters:

- Name – Specify the name of the daemon that you wish to check (e.g. lpd).
- State – Specify whether this check should verify if the daemon is running or stopped.

5 Check folders

5.1 Introduction

In GFI Network Server Monitor, all checks are organised into folders. Folders have properties such as alerts, dependencies and maintenance parameters that are inherited by the checks contained in those folders. This way, it is easy to change an alert or dependency for a whole group of checks from a centralized point. By default, a check inherits properties from the parent folder; however, you can override this setting for individual checks if necessary.



Screenshot 90 - Nested Folders

Nested Folders (Folders contained in other folders) are supported in the Enterprise/Consultant Editions. Nested Folders is a configuration feature which allows you to organize monitoring checks in a deeper hierarchical manner which reflects more closely the specialized monitoring needs of your companies.

Nested folders are not available in the Professional Edition license of GFI Network Server Monitor

Nested folders can also inherit properties from their parent folder.

You can create folders yourself (New > folder…) or you can let the New check wizards (i.e., the 'New Check' or 'Quick Start' wizard) create them automatically for you when new checks are being created. Folders that are created by check wizards are given the names of target computers for which the checks are created.

Folders with the same name cannot exist on the same level. This means that you can have folders with the same name but only if they are located within separate parent folders.

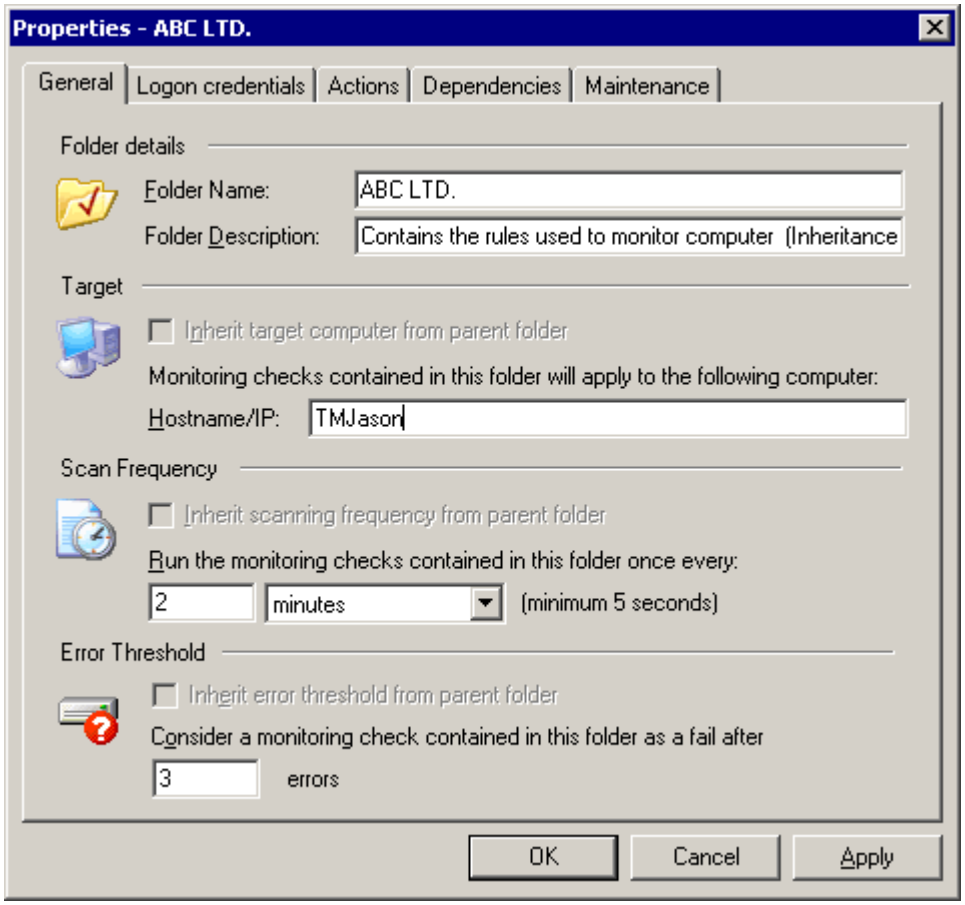
5.2 Creating new folders

To create a folder:

1. Right click on the destination (i.e., where you wish to create the new folder), then select New > Folder. For example, to create a folder within another folder called ZONE1, right click on ZONE1, then go on New > Folder.

To create a folder in root, right click on the 'Monitoring Checks Configuration' node, then go on New > Folder.

After evaluation, you can use the nested folder feature only if you own a Consultant or Enterprise license for GFI Network Server Monitor. If you have purchased a Professional license, you can create folders but only under the root folder "Monitoring Checks Configuration".



Screenshot 91 - Folder properties dialog: General Tab

2. Specify the folder details; i.e. folder name (e.g. TMJASON) and folder description.

3. Configure the rest of the folder properties in the same way as is done for the monitoring checks properties. For the configuration instructions, refer to the 'Configure monitor check properties' section in the 'Configuring GFI Network Server Monitor' chapter.

4. Click on 'OK' to save the configuration settings and exit the folder properties dialog.

Example: Configuring the target computer parameter

1. Right click on the folder to be configured and select properties.. By default the check properties dialog will open up in the 'General' tab.

2. Specify the target computer name or IP address (e.g. TMJASON or 192.168.1.100) in the 'Target' section.

3. Click on 'OK' to accept the configuration settings and exit the folder properties dialog.

5.3 Configure properties of existing folders

To configure properties of an existing folder, right click on the folder and select 'Properties'. For other configuration instructions, please refer to the 'Configure monitor check properties' section in the 'Configuring GFI Network Server Monitor' chapter.

5.4 Deleting folders

To delete a particular folder, right click on the folder name and select 'Delete'.

Folder deletion cannot be undone. We recommend that you back up your current GFI Network Server Monitor configuration before proceeding with the deletion of folders. This will allow you to restore your previous configuration, thus recovering deleted folders if needed. To back up your current configuration, go on File > Export Configurations. For more information on configuration backups, refer to the 'Export configurations' section in the 'Other features' chapter of this manual.

5.5 Moving folders

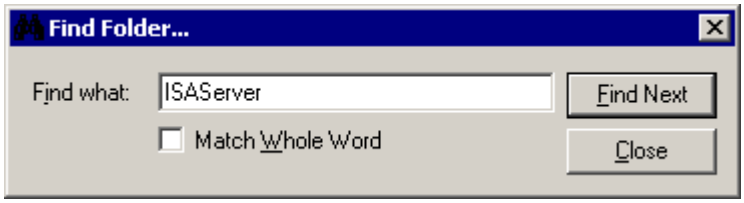
To move a folder:

1. Right click on the folder that you wish to move and select 'Cut'.

2. Go on the preferred destination and select 'Paste'.

You can also drag and drop the folder from its present to target location.

5.6 Searching for folders



Screenshot 92 - Find folder dialog

The Find Folder tool allows you to search and locate folders in your folder tree. To start a folder search:

1. Right click on the 'Monitoring Checks Configuration' node and select 'Find Folder'.

2. In the Find Folder dialog, specify the required search string. This can be the complete folder name as well as any character(s) which are present in the name of the required folder. To locate only those folder names which match exactly the specified criteria, select the option 'Match Whole Word'.

3. Click on ‘Find Next’ to start the search. The Find Folder tool will identify and highlight every occurrence matching the specified string. Keep clicking on ‘Find Next’ until you locate the required folder.

4. To stop the search, click on ‘Close’.

6 Monitoring checks status

6.1 Introduction

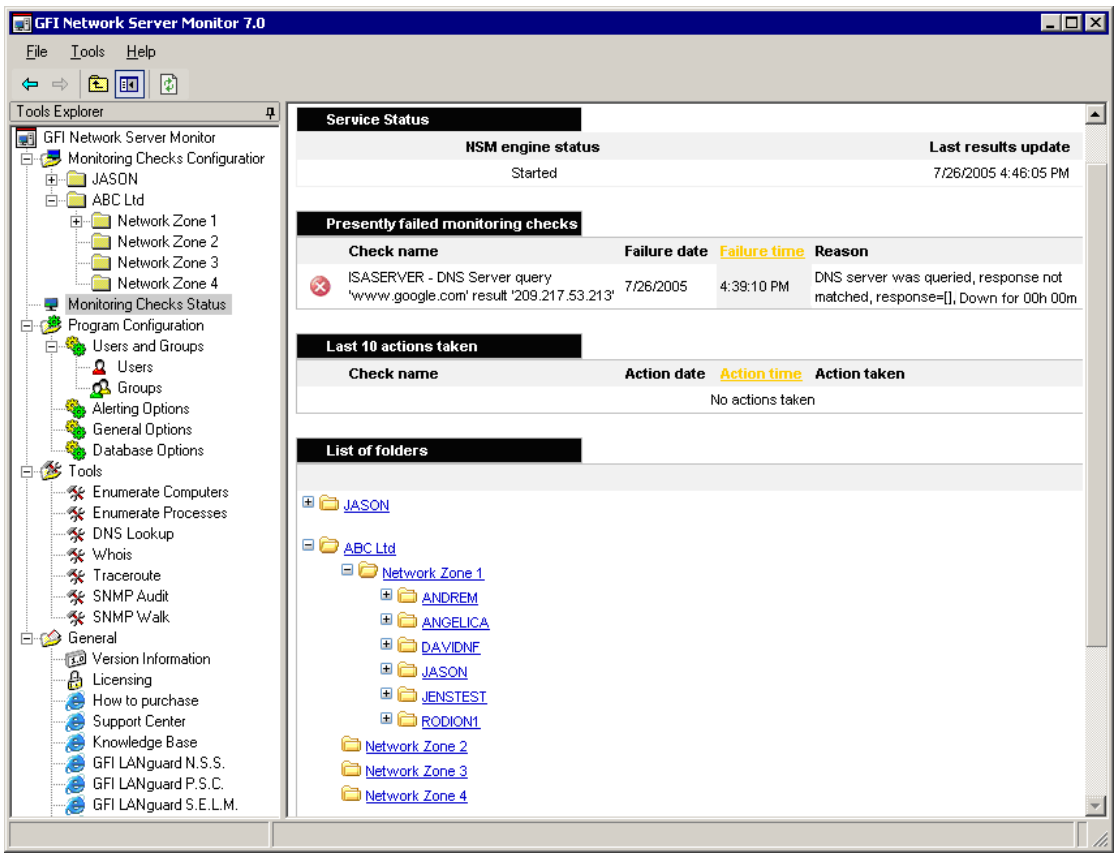
You can view the current state of monitoring checks in three ways:

1. From the GFI Network Server Monitor configuration, by clicking on the 'Monitoring Check Status' node. For more information, refer to the 'Viewing the state of checks from the GFI N.S.M. configuration' section in this chapter.

2. From a dedicated application called GFI N.S.M. 7 Activity Monitor. This application is automatically installed with GFI Network Server Monitor and can be launched by going on Start > Programs > GFI Network Server Monitor 7 > GFI N.S.M. 7 Activity Monitor. For more information, refer to the 'Viewing the state of checks from the GFI NSM Activity Monitor' section in this chapter.

3. From your Internet Explorer, through the remote web monitor included in GFI Network Server Monitor. For more information, refer to the 'Viewing the state of checks remotely' section in this chapter.

6.2 Viewing the state of checks from the GFI N.S.M. configuration



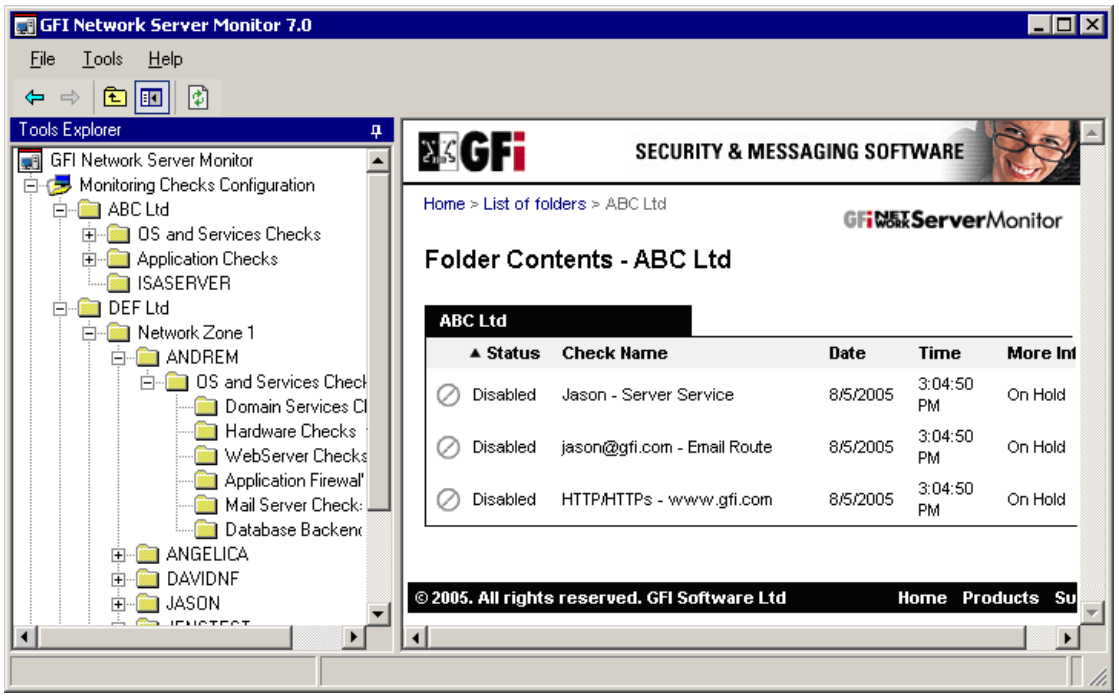
Screenshot 93 - Monitoring Checks status home page

GFI Network Server Monitor allows you to view the state of monitor checks directly from its configuration program. To view this information click on the 'Monitor Checks Status' node. This by default, opens the Status Monitor "Home" page in the events (right-hand-side) window. The home page displays all "Failed" checks as well as the last 10 actions that GFI Network Server Monitor has performed. The information on display also includes:

- The current state of the monitoring engine (i.e., started or stopped).
- The date and time when each check failed.
- The reason for this failure (e.g., if a required file is not found during a 'file existence check', the reason displayed would be 'File does not exist').

The icon on the left-hand-side of listed checks indicates the relative check status. For more information on these icons, refer to the 'Check State Indicators' section in this chapter.

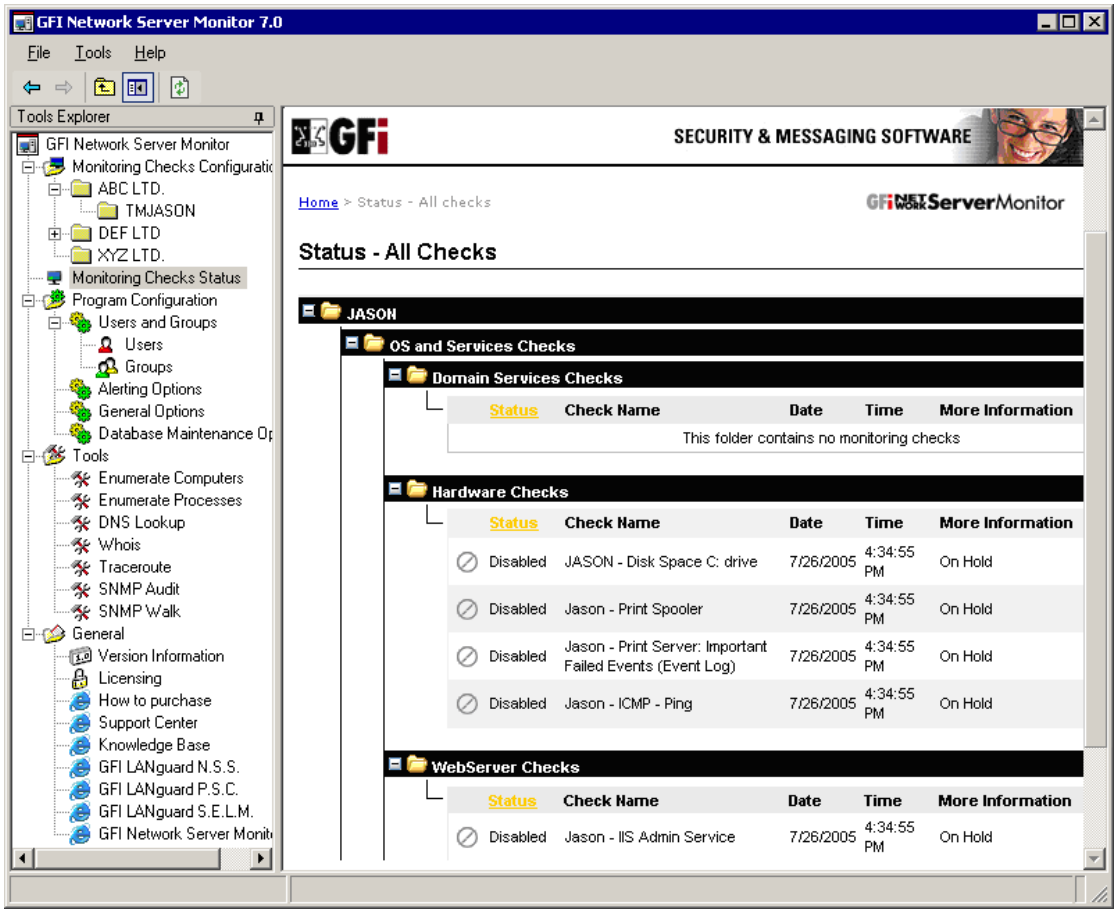
The Status Monitor home page also includes a list of all the folders present in GFI Network Server Monitor. This list is displayed at the bottom of the page.



Screenshot 94 - The Folder contents page

To view the status of the checks contained in a folder, click on the folder name. This will open the folder contents page, which shows information on the checks located in that folder. This information includes the present status of these checks. To select another folder, return to the home page by clicking on the 'Home' link located at the top-left of this page.

Viewing all the checks



Screenshot 95 - All checks page

To view the status of all checks in GFI Network Server Monitor, click on the 'Status – All checks' link located at the top of the Status Monitor home page. This will display a list of all the checks, grouped under their respective folder.

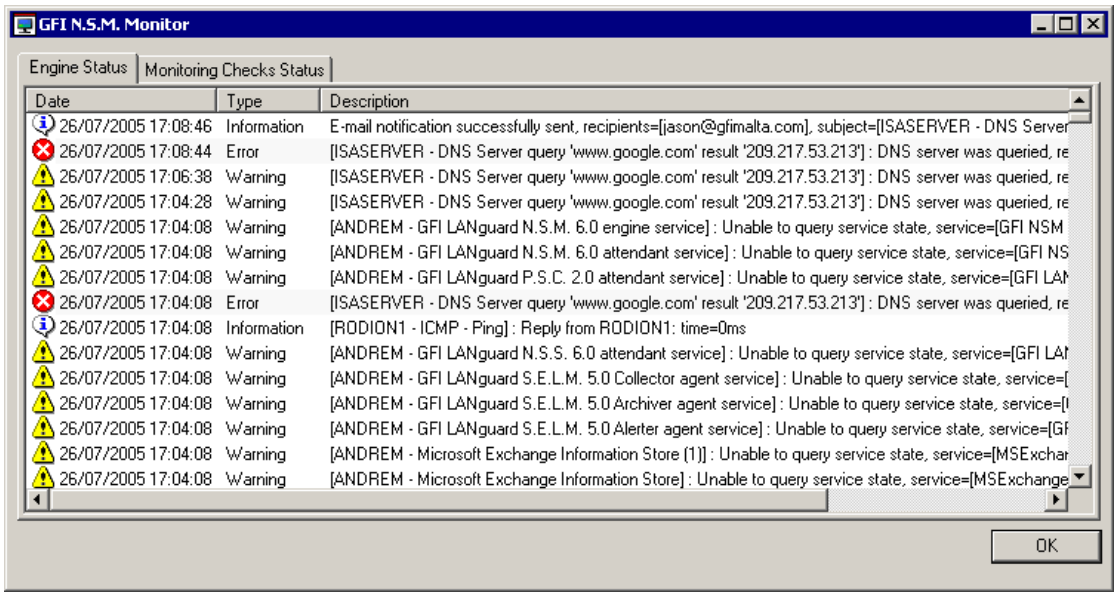
Screenshot 96 - Nested Folders

You can expand or collapse the contents of a folder by clicking on ⊞ or ⊟ respectively.

TIP: Although the view is automatically refreshed at timed intervals, you can refresh the displayed information by right clicking on the page and selecting 'Refresh'.

6.3 Viewing the state of checks from the GFI N.S.M. Activity Monitor

GFI Network Server Monitor ships with an Activity Monitor which enables you to view the status of the monitoring engine and monitoring checks. This activity monitor is automatically installed with GFI Network Server Monitor and thus it can only be used from the computer where this software is installed. To launch the Activity Monitor, go on Start > Programs > GFI Network Server Monitor 7 > GFI N.S.M. 7 Activity Monitor.

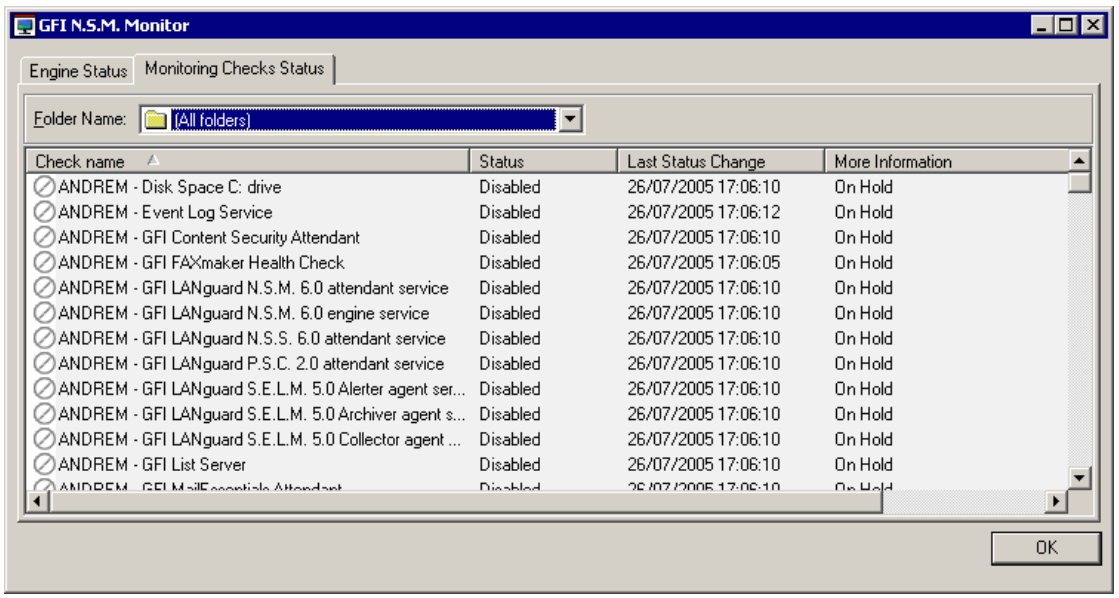

GFI N.S.M. Monitor
Engine Status
Monitoring Checks Status
Date
Type
Description
26/07/2005 17:08:46 Information E-mail notification successfully sent, recipients=[jason@gfimalta.com], subject=[ISASERVER - DNS Server
26/07/2005 17:08:44 Error [ISASERVER - DNS Server query 'www.google.com' result '209.217.53.213'] : DNS server was queried, re
26/07/2005 17:06:38 Warning [ISASERVER - DNS Server query 'www.google.com' result '209.217.53.213'] : DNS server was queried, re
26/07/2005 17:04:28 Warning [ISASERVER - DNS Server query 'www.google.com' result '209.217.53.213'] : DNS server was queried, re
26/07/2005 17:04:08 Warning [ANDREM - GFI LANguard N.S.M. 6.0 engine service] : Unable to query service state, service=[GFI NSM
26/07/2005 17:04:08 Warning [ANDREM - GFI LANguard N.S.M. 6.0 attendant service] : Unable to query service state, service=[GFI NS
26/07/2005 17:04:08 Warning [ANDREM - GFI LANguard P.S.C. 2.0 attendant service] : Unable to query service state, service=[GFI LA
26/07/2005 17:04:08 Error [ISASERVER - DNS Server query 'www.google.com' result '209.217.53.213'] : DNS server was queried, re
26/07/2005 17:04:08 Information [RODION1 - ICMP - Ping] : Reply from RODION1: time=0ms
26/07/2005 17:04:08 Warning [ANDREM - GFI LANguard N.S.S. 6.0 attendant service] : Unable to query service state, service=[GFI LA
26/07/2005 17:04:08 Warning [ANDREM - GFI LANguard S.E.L.M. 5.0 Collector agent service] : Unable to query service state, service=[
26/07/2005 17:04:08 Warning [ANDREM - GFI LANguard S.E.L.M. 5.0 Archiver agent service] : Unable to query service state, service=[
26/07/2005 17:04:08 Warning [ANDREM - GFI LANguard S.E.L.M. 5.0 Alerter agent service] : Unable to query service state, service=[GF
26/07/2005 17:04:08 Warning [ANDREM - Microsoft Exchange Information Store (1)] : Unable to query service state, service=[MSExchar
26/07/2005 17:04:08 Warning [ANDREM - Microsoft Exchange Information Store] : Unable to query service state, service=[MSExchange
OK

Screenshot 97 - Engine Status tab

The GFI N.S.M. Activity Monitor opens up by default in the 'Engine Status' tab. This tab displays all the information related to the activity of the monitoring engine. Such information includes:

- The date and time of the activity.
- The type of activity (e.g., Error, Warning, etc.).
- A description of the event.

Icons on the left-hand-side of each event graphically indicate the event type. These icons help you to easily identify the status without having to read the 'Type' column details.


GFI N.S.M. Monitor
Engine Status
Monitoring Checks Status
Folder Name:
(All folders)
Check name
Status
Last Status Change
More Information
ANDREM - Disk Space C: drive Disabled 26/07/2005 17:06:10 On Hold
ANDREM - Event Log Service Disabled 26/07/2005 17:06:12 On Hold
ANDREM - GFI Content Security Attendant Disabled 26/07/2005 17:06:10 On Hold
ANDREM - GFI FAXmaker Health Check Disabled 26/07/2005 17:06:05 On Hold
ANDREM - GFI LANguard N.S.M. 6.0 attendant service Disabled 26/07/2005 17:06:10 On Hold
ANDREM - GFI LANguard N.S.M. 6.0 engine service Disabled 26/07/2005 17:06:10 On Hold
ANDREM - GFI LANguard N.S.S. 6.0 attendant service Disabled 26/07/2005 17:06:10 On Hold
ANDREM - GFI LANguard P.S.C. 2.0 attendant service Disabled 26/07/2005 17:06:10 On Hold
ANDREM - GFI LANguard S.E.L.M. 5.0 Alerter agent ser... Disabled 26/07/2005 17:06:10 On Hold
ANDREM - GFI LANguard S.E.L.M. 5.0 Archiver agent s... Disabled 26/07/2005 17:06:10 On Hold
ANDREM - GFI LANguard S.E.L.M. 5.0 Collector agent ... Disabled 26/07/2005 17:06:10 On Hold
ANDREM - GFI List Server Disabled 26/07/2005 17:06:10 On Hold
OK

Screenshot 98 - Monitoring Check Status tab

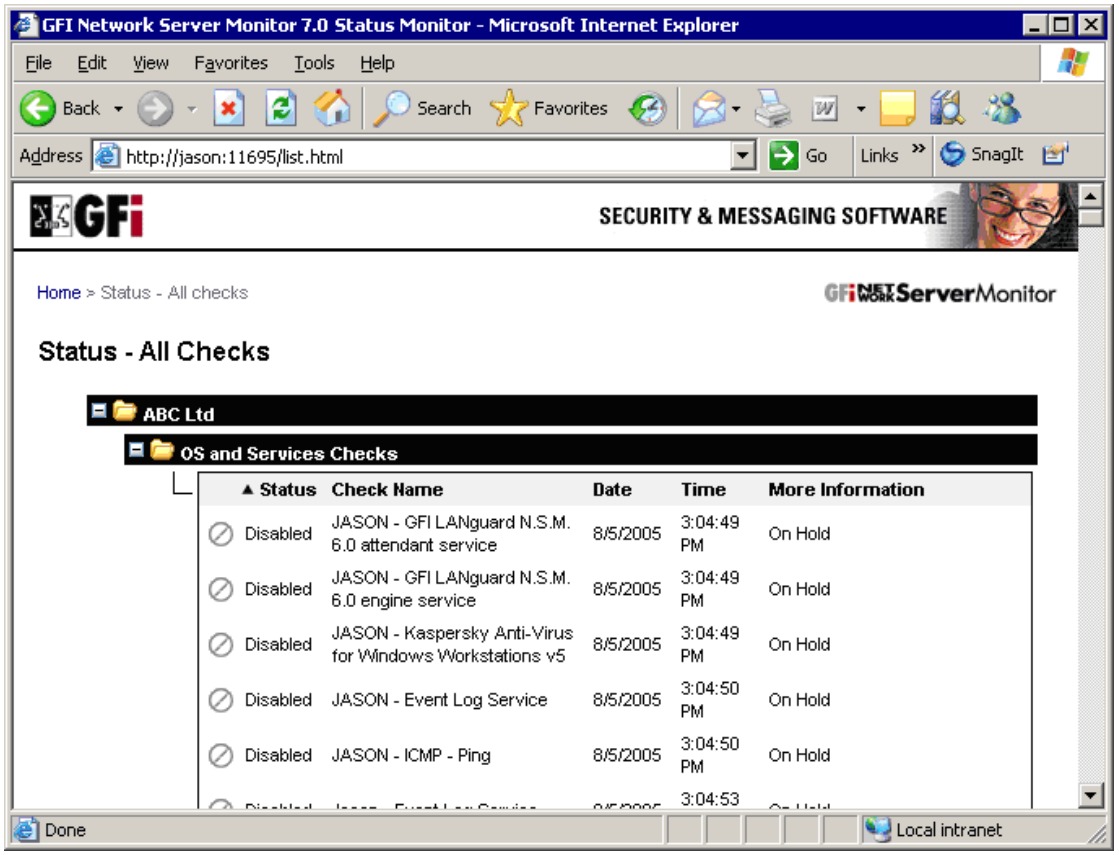
The GFI NSM Activity Monitor also includes a 'Monitoring Checks Status' tab. This displays information on monitoring checks such as the current state and the date/time of the last change in state. Since checks are stored in folders, you can also choose to see only the checks which are contained in a particular folder of interest. Folders are selected from the 'Folder Name' drop

down included at the top of the dialog. For example, to see all of monitoring checks which are configured in GFI Network Server Monitor irrespective of which folder they are contained in, select "(All folders)" from the available drop down list.

6.4 Viewing the state of checks from a web browser

GFI Network Server Monitor also ships with a remote web monitor. This allows you to remotely view the status of checks via Internet Explorer over a network or Internet. Through the remote web monitor you can examine the status of your network from virtually anywhere, both within and outside the company's building. By default, the remote web monitor supports two views. These are the "Normal" view and the "Mobile Device" view.

Normal view


GFI Network Server Monitor 7.0 Status Monitor - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://jason:11695/list.html
Go Links SnagIt
GFI
SECURITY & MESSAGING SOFTWARE
Home > Status - All checks
GFI NetworkServerMonitor
Status - All Checks
ABC Ltd
OS and Services Checks
Status Check Name Date Time More Information
Disabled JASON - GFI LANguard N.S.M. 6.0 attendant service 8/5/2005 3:04:49 PM On Hold
Disabled JASON - GFI LANguard N.S.M. 6.0 engine service 8/5/2005 3:04:49 PM On Hold
Disabled JASON - Kaspersky Anti-Virus for Windows Workstations v5 8/5/2005 3:04:49 PM On Hold
Disabled JASON - Event Log Service 8/5/2005 3:04:50 PM On Hold
Disabled JASON - ICMP - Ping 8/5/2005 3:04:50 PM On Hold
Done
Local intranet

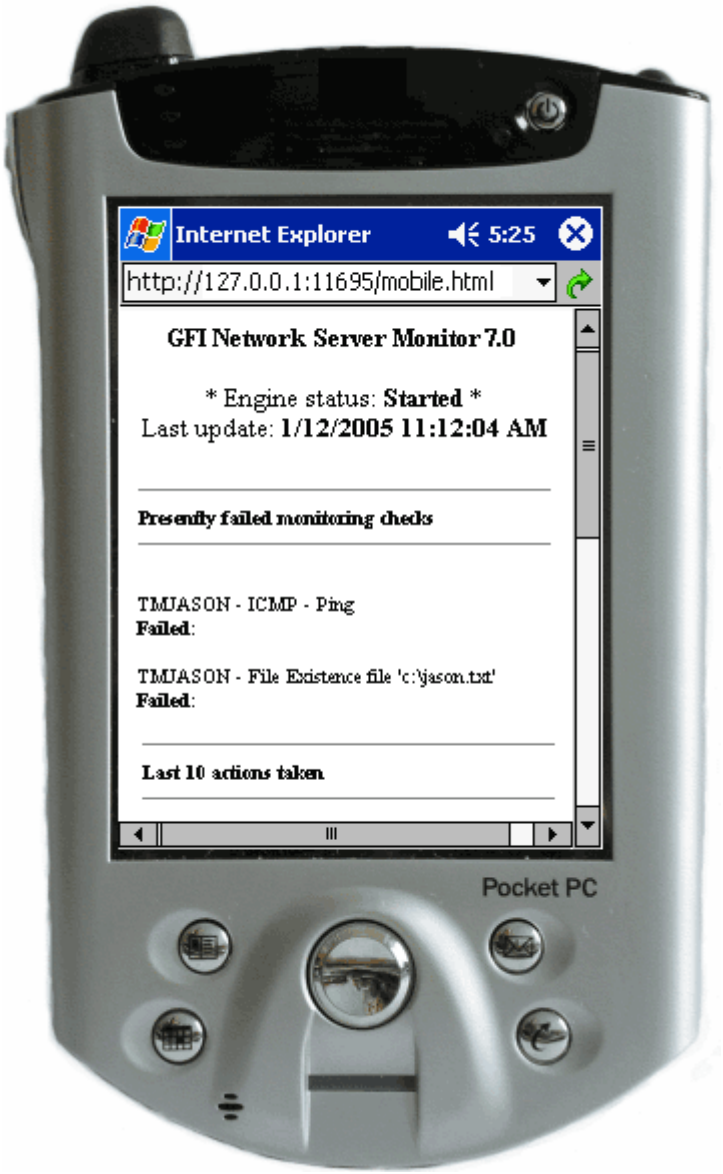
Screenshot 99 - Remote Monitor: All checks page

The "Normal" view displays information in a layout structured for viewing on 'normal sized' screens (e.g., computer monitors). To inspect your network status in Normal view, open your Internet Explorer and type in the following URL: *http://<IP address or computer name>:11695/list.html*.

The *<IP address or computer name>* in the URL is the Name/IP of the computer where GFI Network Server Monitor is installed

By default, the normal view opens up in the "All checks" page. This page displays the status of all checks currently configured in GFI Network Server Monitor. The navigation and information layout are identical to those of the 'Monitoring Check status' feature in the configuration program. For more information on how to navigate through the information on display, refer to 'Viewing the state of checks from the GFI NSM configuration' section in this chapter'.

Mobile device view



Screenshot 100 - Monitoring checks status view for mobile devices

The 'Mobile device' view displays information in a layout suitable for viewing on small displays. Such displays are commonly found on small portable devices, for instance mobile phones and PDAs. To inspect your network status in 'Mobile device' view, open your Internet Explorer and type in the following URL: *http://<IP address or computer name>:11695/mobile.html*

In both normal and mobile device view, the communication between the web browser (i.e., Internet Explorer) and the computer running GFI Network Server Monitor is carried out via port 11695.

By default, GFI Network Server Monitor includes a small footprint web server which can be set up from the configuration. This avoids having to install and configure IIS to display your network status information on screen.

For security reasons, we recommend the use of Microsoft IIS web server for accessing and viewing the state of your monitoring checks. For further information on IIS web server setup, refer to the 'Configuring IIS as the web server' section in the 'General Options' chapter.

The default port used can be customized from Configuration > General Options > Web Server.

6.5 Check state indicators

Check state indicators are images which graphically define the current state of your monitoring checks. The following is a list of states which any monitoring check can have:

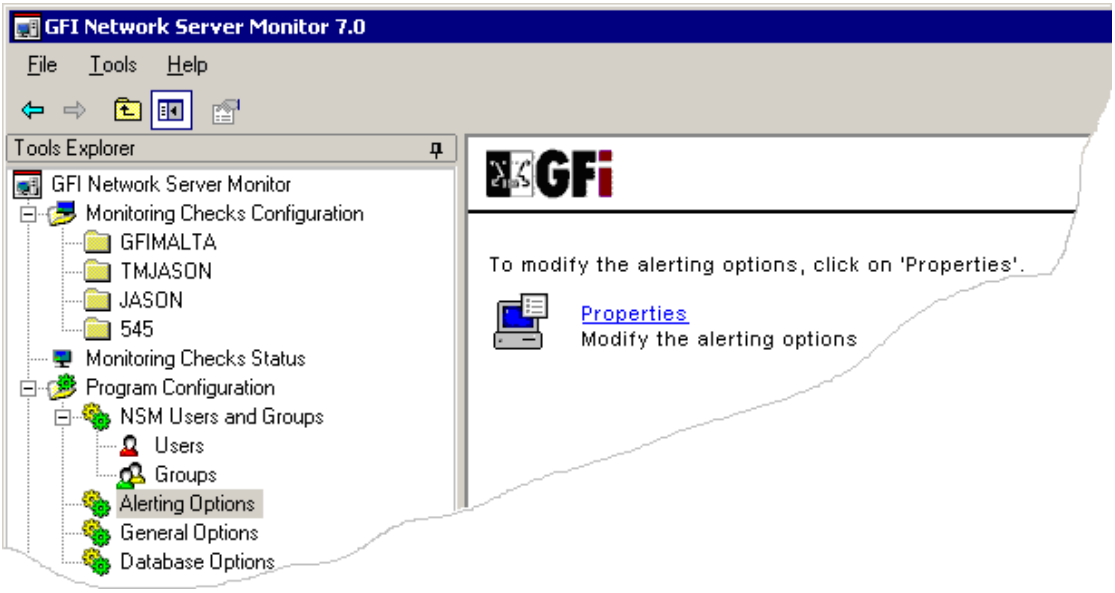
- Queued – Check is waiting to be processed.
- Success – Check successful.
- Failure – Check not successful/failed. A check is not marked as failed on the first unsuccessful result. At first, the check is placed under a 'Pending Failure' state. After some time, the check is re-run to verify that the check is indeed failing. Once a failure threshold (configured in the check/folder properties) is exceeded, the check is deemed to be definitely failing and placed in the "Failure" state. For more information on errors and error threshold parameters, please refer to the 'Configure monitor check properties' chapter in this manual.
- Disabled – User configured this check not to be run. For more information on how to enable/disable checks, please refer to the 'Enable or disable checks' section in this manual.
- Not Monitored – Check cannot be processed by the GFI Network Server Monitor engine. This occurs when the monitoring service is stopped or when a check requires a particular service (e.g., the SNMP or WMI service) which is not available on the target computer.
- Server in Maintenance – Check has been executed against a target computer during its maintenance hours. When this happens no actions are triggered (E.g., no alerts are sent).
- Failure by Dependee – The check was not executed because a dependency check has already failed, e.g., if the router cannot be pinged, do not check that services running on that router are working.
- Pending failure – Check has failed but did not exceed the error threshold level required to move a check from the 'Pending Failure' state to the 'Failed' state.
- Uncertain/Processing Error – Indicates that the result of a monitoring check cannot be clearly determined (i.e., cannot be directly classified as Success or Failure). For example, the engine tries to run a disk space monitoring check against a target computer which is switched off; GFI Network Server Monitor is not able to determine the available disk space due to a situation outside the context of that check. Other situations which can cause an uncertain result are timeouts over a slow network or firewall blocking the communication between GFI Network Server Monitor and the target computer. When such situations occur, monitoring checks are placed in an uncertain state.

When a check is in an uncertain state, no actions are generated (i.e., no alerts, etc.)

Use the General Options > 'Uncertain Results' tab to configure GFI Network Server Monitor on how to treat uncertain results. Checks in an uncertain state can be transformed into Success/Failed checks state depending on your monitoring needs.

7 Global alerting options

7.1 Introduction



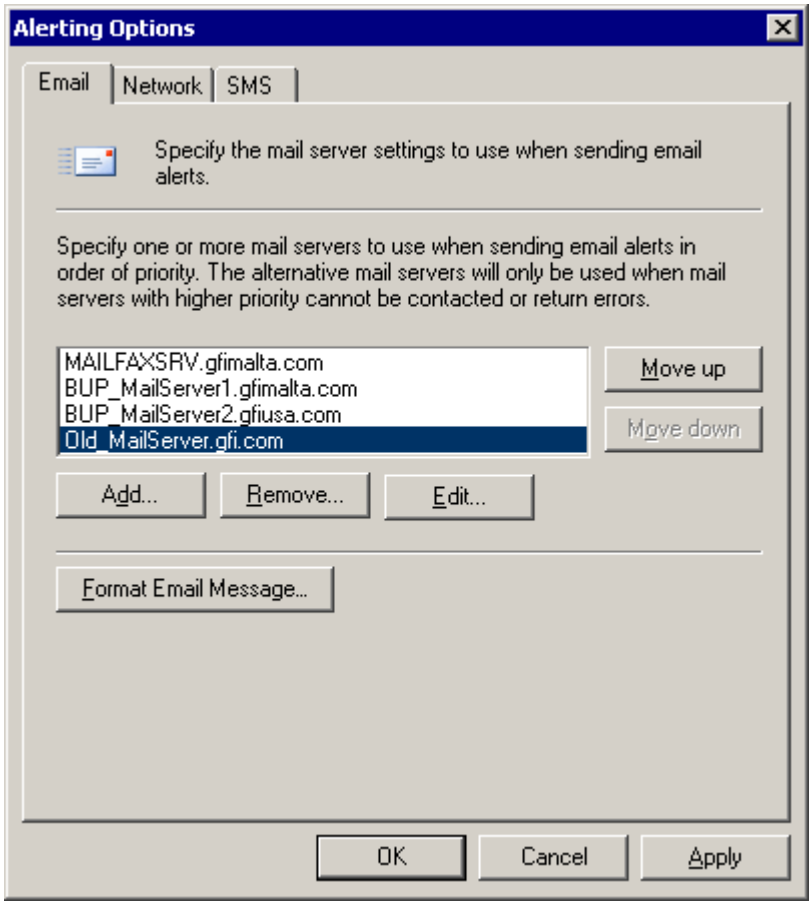
Screenshot 101 - 'Alerting Options' node

The 'Alerting Options' node contains the general alerting parameters required by GFI Network Server Monitor for sending Email, Network and SMS/Pager alerts. From this node you can:

- Specify which mail servers can be used to send email alerts. In addition you can format and define the contents of the email message.
- Specify SMS/Pager settings and format the message to be used when sending SMS/Pager alerts.
- Format the message template used for email, network and sms/pager alerts.

7.2 Mail server settings

GFI Network Server Monitor needs to know which mail server(s) can be used to send email alerts. Although alerts can be sent through only one mail server, you can specify alternative servers which can be used in the event of a mail server failure.



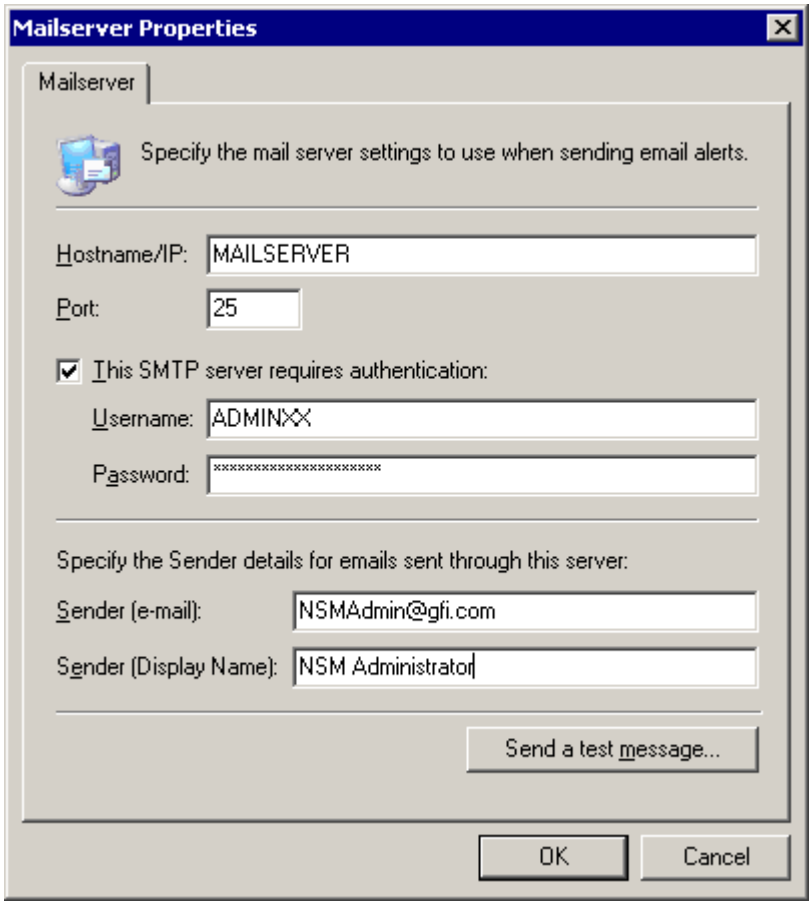
Screenshot 102 - Email Alerts configuration dialog

By default, the server at the top of the mail servers list has the highest priority and is used to send email alerts. If this server is not available, GFI Network Server Monitor automatically switches to the next mail server in the list. This continues until an available mail server is found and the email alert is successfully sent.

Sort the mail servers list in ascending order of priority. This means that the server at the top of the list has highest priority and is the first one to be used. To change the priority of a selected server, click on 'Move Up' or 'Move Down' accordingly.

7.2.1 Adding a Mail server

1. Right click on the 'Alerting Options' node and select 'Properties'. The alerting properties will open by default in the Email Alerts configuration dialog (i.e., Email tab).



Screenshot 103 - Mail server propertiesdialog

2. Click on 'Add' and specify the following parameters in the Mail server properties dialog:

- Hostname/IP - Specify the Hostname (e.g. Mailserver) or IP address (e.g. 192.168.1.200) of the Mail server to be used.
- Port - Specify the TCP communication port to be used for the transmission. (This parameter is set by default to SMTP-port 25)
- This SMTP server requires authentication – Select this option if your SMTP server requires authentication to send email messages. Specify the logon credentials in the provided fields.
- Sender (email) - Specify the email account which will be used when sending emails from the specified SMTP server (e.g., nsmadmin@gfi.com).
- NOTE: All alerts generated by GFI Network Server Monitor will be sent via the specified email account.
- Sender (Display Name) – Specify a display name for the Sender's email account.

To test this configuration, click on 'Send a test message'. This function makes use of the specified mail server parameters to send a test email to the specified email address.

3. Click on 'OK' to close the mail server properties dialog.
4. To change the priority of the configured mail server, click on 'Move Up' or 'Move Down'.
5. Click on 'OK' to save these settings and exit the Email Alerts configuration dialog.

7.2.2 Edit existing mail server details

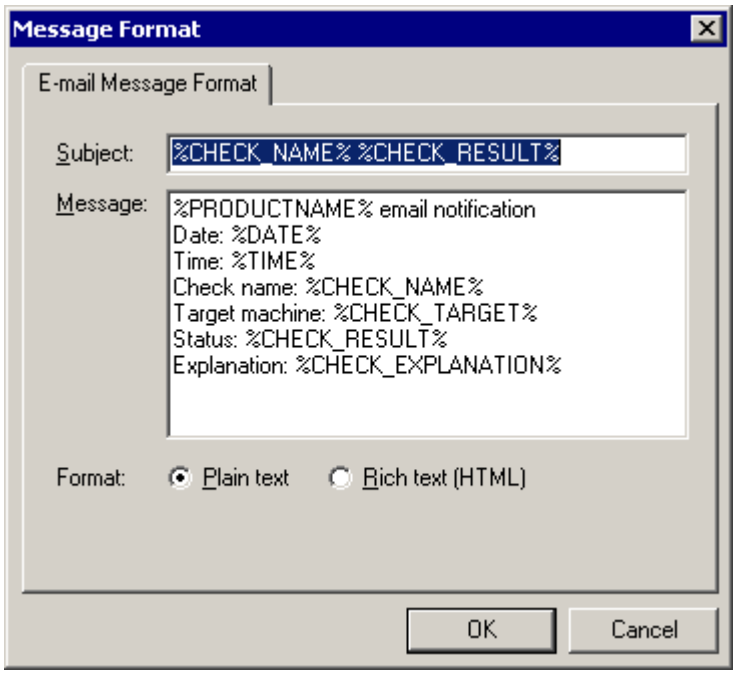
To change configured mail server details:

1. Right click on the 'Alerting Options' node and select 'Properties'. The alerting properties will open by default in the Email Alerts configuration dialog (i.e., Email tab).

2. Click on 'Edit' and make the required configuration changes. For more details on mail server configuration, refer to the 'Adding a mail server' section in this chapter.

Formatting the email message

The alert message can contain manually inputted text (e.g., Alert by NSM), text from system variables (e.g., %CHECK_RESULT%), or a combination of both (e.g., Alert Message from %CHECK_NAME% check).



Screenshot 104 - Format Email Message

For more information on variables and message template formatting, please refer to the 'Message Template' section in this chapter.

To make changes in the email message:

1. Right click on the 'Alerting Options' node and select 'Properties'. The alerting properties will open by default in the Email Alerts configuration dialog (i.e., Email tab).

2. Click on 'Format Email Message' and specify the following parameters:

- Subject – Specify the text to be included in the message's subject field. By default, the subject field is set to include the contents of the %CHECK_NAME% variable (i.e., the name of the monitoring check that triggered the alert).
- Message – Specify the contents of the message body. We recommend that in the message body, you include details related to the event which triggered the alert. By default the message body includes the following information:
  - %PRODUCTNAME% email alert – Product short name (i.e. GFI N.S.M.)
  - Date: %DATE% - The date when the alarm was triggered.
  - Time: %TIME% - The time when the alarm was triggered.
  - Check name: %CHECK_NAME% - The monitor check which triggered the alarm.
  - Target computer: %CHECK_TARGET% - The computer on which the event occurred.
  - Status: %CHECK_RESULT% - The current state of the monitor check which triggered the event (E.g., Failed

- Explanation: %CHECK_EXPLANATION% - Details on the result of the executed check.

» *Format* - Define the message format by selecting one of the following:

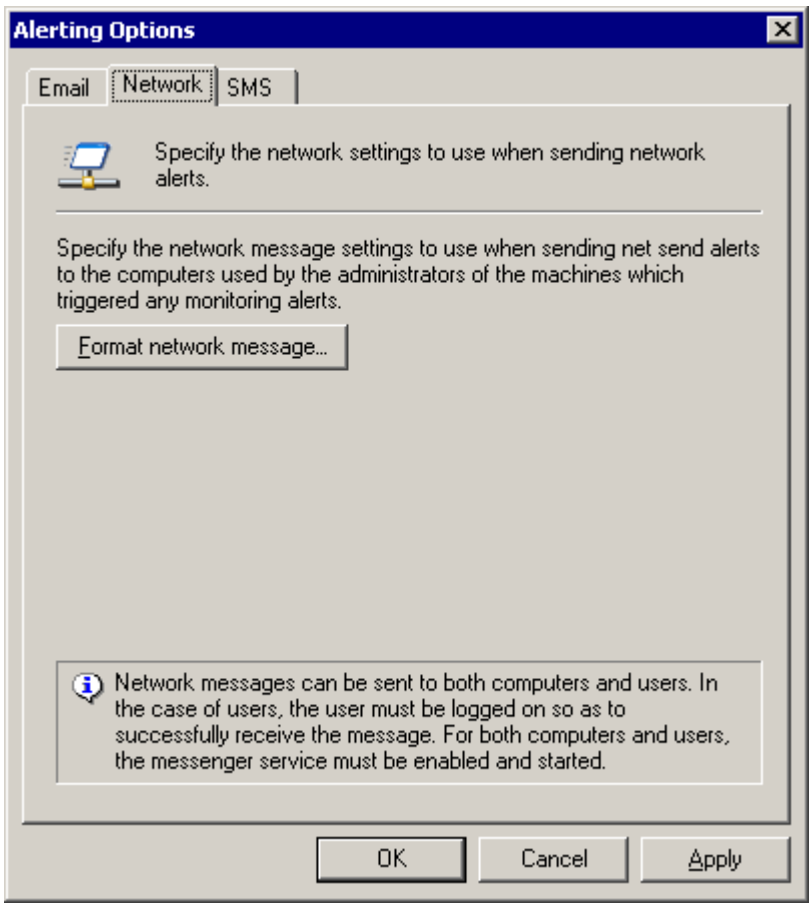
- *Plain text* – Send the email in plain text.
- Rich text – Send the email in HTML.

For more information on variables and message templates, please refer to the 'Message Template' section in this chapter.

7.3 Global settings for network alerts

GFI Network Server Monitor makes use of 'net send' to send network alerts. Make sure that you enable the 'Messenger' service (svchost.exe -k netsvcs) on the computers which will send and receive network messages.

Network alerts are configured from the user properties. For more information on the configuration of network messaging, please refer to the 'Configure user properties' section in the 'Users and Groups' chapter.


Alerting Options
Email
Network
SMS
Specify the network settings to use when sending network alerts.
Specify the network message settings to use when sending net send alerts to the computers used by the administrators of the machines which triggered any monitoring alerts.
Format network message...
Network messages can be sent to both computers and users. In the case of users, the user must be logged on so as to successfully receive the message. For both computers and users, the messenger service must be enabled and started.
OK
Cancel
Apply

Screenshot 105 - Network Alerts Properties

Format network message

1. Right click on the 'Alerting Options' node and select Properties.
2. Click on the 'Network' tab and then click on 'Format Network Message'.

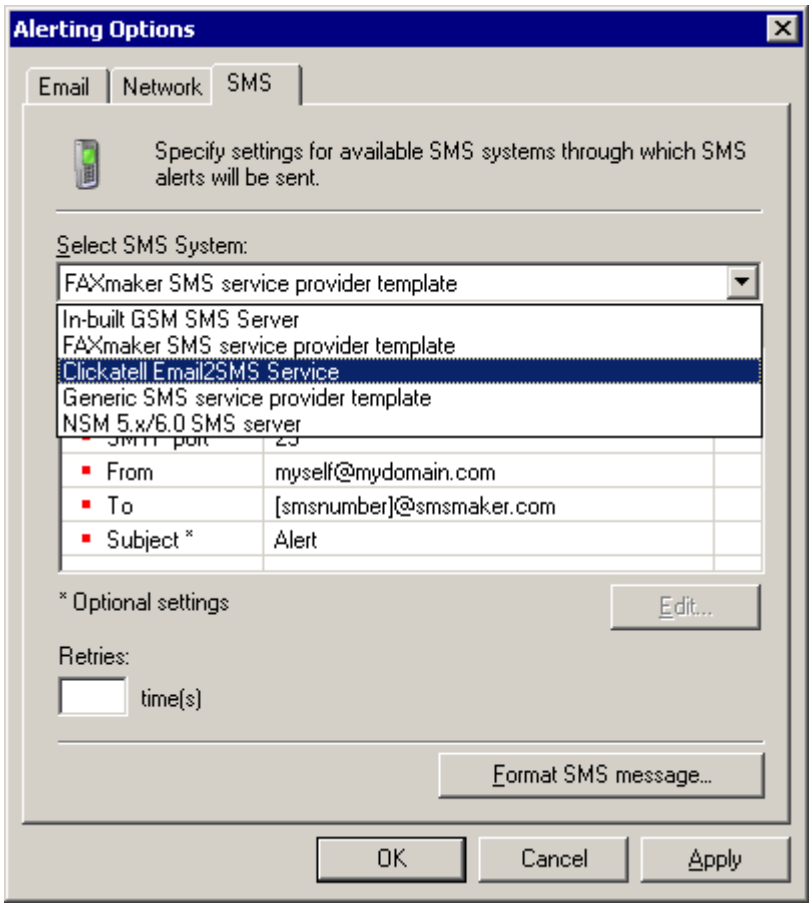
3. Make the required changes to the message. The formatting of this message is identical to that of the email message.

4. Click on 'OK' to accept these changes.

For more information on variables and message templates, please refer to the 'Message Template' section in this chapter.

7.4 Global settings for SMS/pager alerts

This section is only applicable for advanced users. We cannot guarantee that GFI Network Server Monitor will work with any SMS provider. Before attempting any such configuration, ensure that you have obtained the correct information from your SMS service provider.



Screenshot 106 - SMS Alerts dialog

Out of the box GFI Network Server Monitor can relay SMS alerts through the:

- In-built GSM SMS Server
- GFI FAXmaker SMS service provider template
- Clickatell Email2SMS Service
- Generic SMS service provider templates
- NSM 5.x/6.0 SMS Server.

7.5 In-built GSM SMS Server

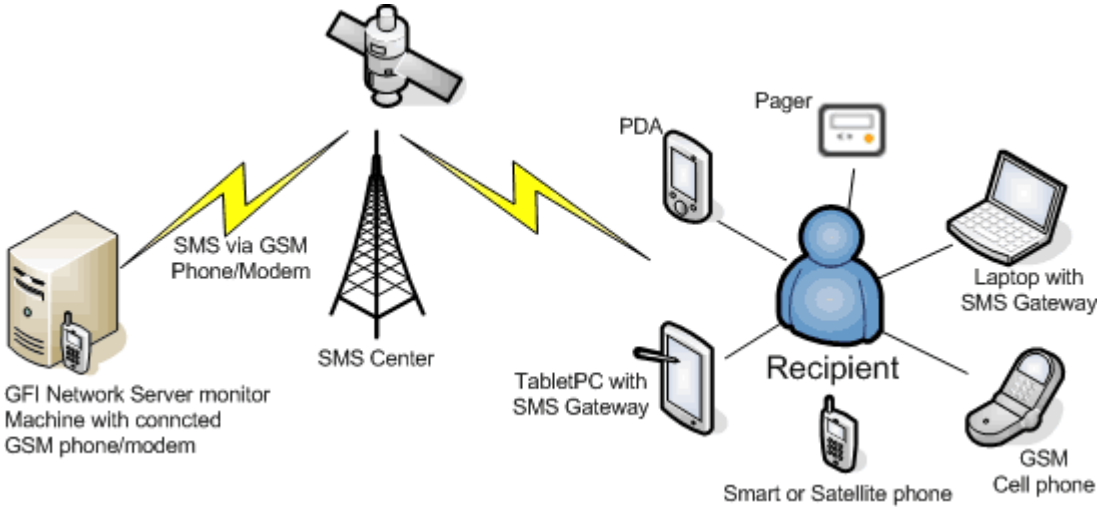
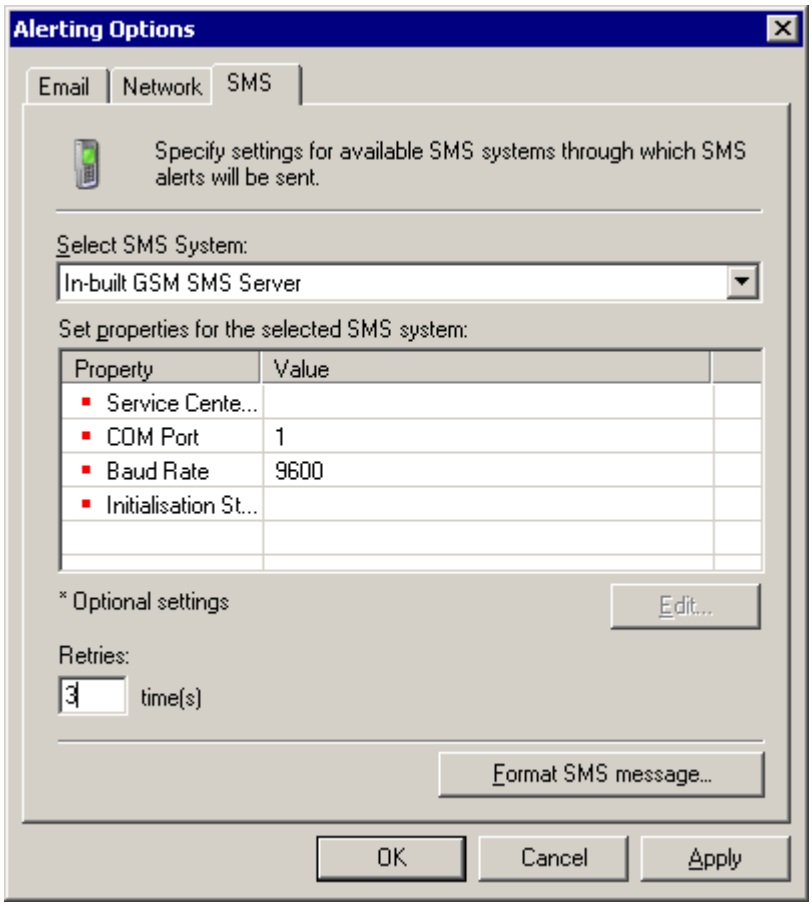


Figure 2 - SMS alert flow via the in-built GSM Server

The in-built GSM SMS Server allows GFI Network Server Monitor to directly send SMS (text) messages through a GSM phone or GSM modem, connected to the computer by serial cable, Infrared or Bluetooth.



Screenshot 107 - The in-built GSM SMS Server properties

Requirements

1. A GSM modem or GSM phone that is capable of processing AT+C commands. This GSM device must be connected to the server running GFI Network Server Monitor.

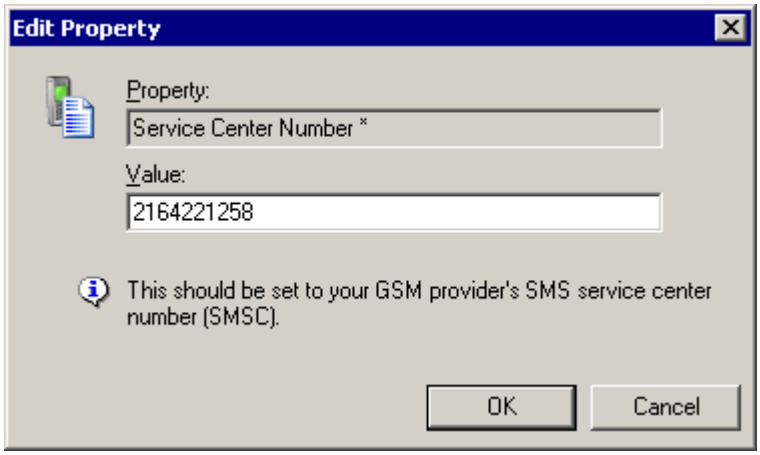
2. Subscription to an SMSC provider.

Configuring the In-built GSM SMS Server

To configure the in-built GSM SMS Server:

1. Right Click on the ‘Alerting Options’ node and select ‘Properties’.

2. Click on the ‘SMS’ tab and from the SMS System dropdown, select ‘In-built GSM SMS Server’.



Screenshot 108 - Edit Property dialog

3. Double click on the property which you want to configure (e.g., Service Center Number) and specify the necessary parameters in the Edit Property dialog.

When configuring properties, always specify the details supplied to you by your SMSC provider. If configuration parameters are not available, ask your provider to supply you with the required information.

The In-built GSM SMS Server requires the following parameters:

- Service Center Number – Specify the number of your provider’s SMS service center (SMSC). This number is supplied by the SMS service provider.
- COM port – Select the COM port where the GSM device (i.e., phone/modem) is connected.
- Baud Rate – Specify the speed at which the communication will take place. Always specify the speed recommended by your SMSC provider.
- Initialization String – (Optional) If required, specify any AT Commands that you wish to send to your modem.

The initialization string is a set of modem AT commands combined into one string (e.g., AT &F &C1 &D2). For a complete list of AT commands, visit http://esvc001164.wic013u.server-web.com/modems/modemstrings.htm

4. In the ‘Retries’ entry box, specify the number of times that the In-built GSM SMS Server will try to send an SMS alert should the first attempt fail.

5. Click on ‘OK’ to save your configuration settings.

7.6 GFI FAXmaker SMS service provider template

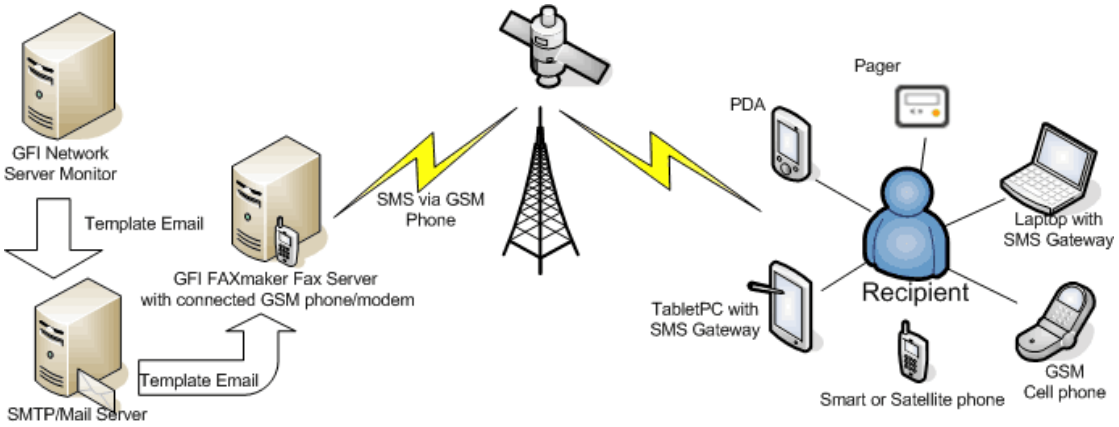


Figure 3 - SMS alert flow via GFI FAXmaker SMS service provider

The GFI FAXmaker SMS Service allows GFI Network Server Monitor to send SMS messages through GFI FAXmaker, market-leading fax server software that allows you to send and receive faxes via your email infrastructure. GFI FAXmaker is also an SMS gateway which allows you to send SMS messages through:

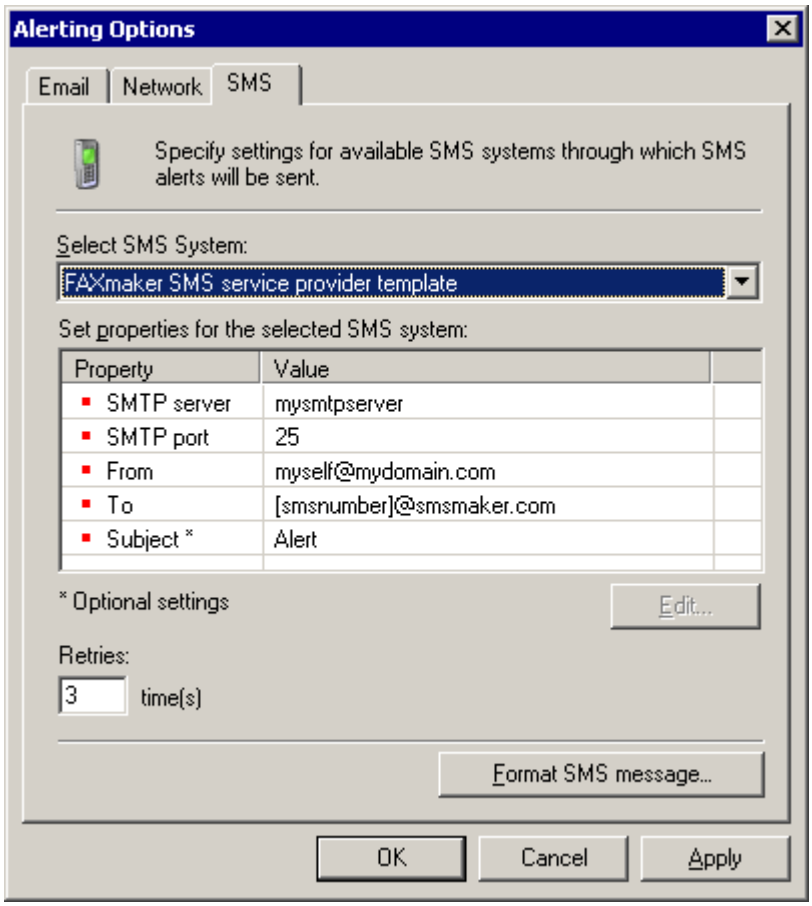
- A GSM phone / modem connected to your fax server.

  Or

- Web-based SMS service providers.

For more information on GFI FAXmaker, visit **http://www.gfi.com/faxmaker/**

Whenever an event triggers an SMS alert, GFI Network Server Monitor sends a "template" email (via SMTP) to the fax server (i.e., GFI FAXmaker). This template email contains all the SMS alert details including the SMS text message and the recipient's number. GFI FAXmaker then converts this email to SMS and sends it to the intended recipient.



Screenshot 109 - FAXmaker SMS service configuration dialog

Requirements

In order to use the FAXmaker SMS service, you must have:

1. GFI FAXmaker installed and configured for SMS messaging. For more information on how to configure the SMS gateway on GFI FAXmaker refer to 'The SMS Gateway' chapter of the GFI FAXmaker manual. You can download the GFI FAXmaker manual from **http://www.gfi.com/downloads/downloads.aspx?pid=FAX&lid=en**

2. A supported GSM phone/modem connected to the GFI FAXmaker fax server computer or a subscription to a supported web-based SMS provider.

Configuring the FAXmaker SMS service

To configure the FAXmaker SMS Service:

1. Right click on the 'Alerting Options' node and select 'Properties'.

2. Click on the 'SMS' tab and from the SMS System dropdown, select 'FAXmaker SMS Service provider template'.

3. Double click on the property which you want to configure (e.g., SMTP server) and specify the relative parameters in the Edit Property dialog.

The FAXmaker SMS Service requires the following parameters:

- SMTP server – Specify the name of the SMTP server through which GFI Network Server Monitor will send the template email to GFI FAXmaker.
- SMTP port – Specify the SMTP port through which the transmission will take place. By default this parameter is set to 25 (i.e., default SMTP port).
- From – Specify the account from where the template email will be sent. Format this parameter as follows: <name>@<mydomain.com>
- To – (Leave as default) This is the email address on which GFI FAXmaker will receive the template emails to be converted to SMS (i.e., [smsnumber]@smsmaker.com). This parameter includes variable [smsnumber] which is substituted to the number of the SMS recipient when the template email is generated. For example, if an SMS must be sent to a recipient with number 88885555, the email is sent on 8888555@smsmaker.com. GFI FAXmaker will then send the SMS on the number specified in the email address.
- Subject* - (Optional parameter) Specify the text which you want to include in the template email's subject field.

4. In the 'Retries' entry box, specify the number of times that the FAXmaker SMS service will try to send an SMS alert should the first attempt fail.

5. Click on 'OK' to save your configuration settings.

7.7 Clickatell Email2SMS Service

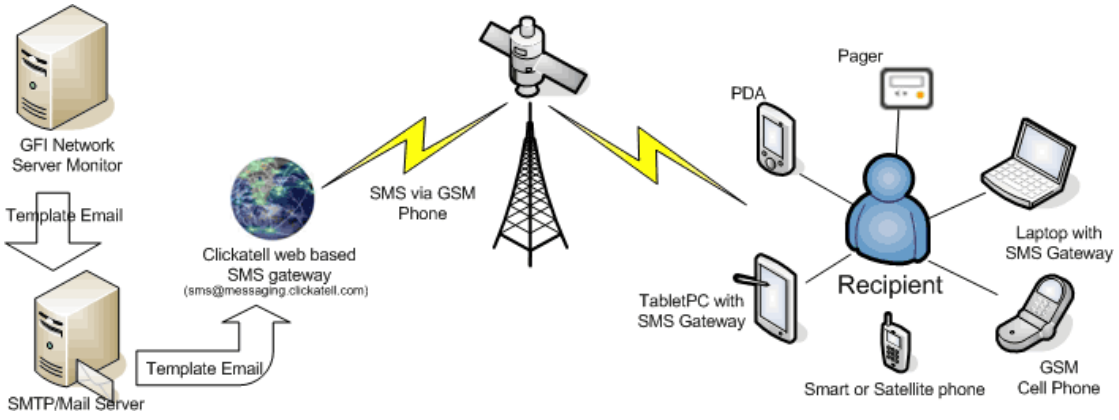
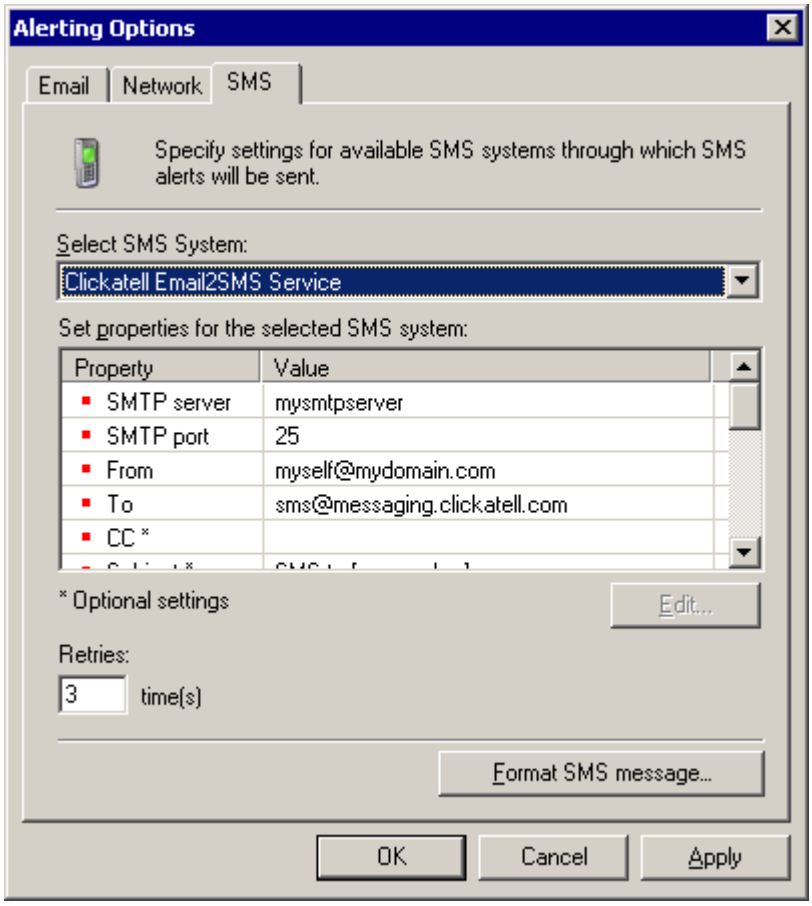


Figure 4 - SMS alert flow via a Clickatell Email to SMS service

The Clickatell Email2SMS Service allows GFI Network Server Monitor to relay SMS (text) alerts via Clickatell, a web-based SMS service which sends SMS messages worldwide.

Whenever an event triggers an SMS alert, GFI Network Server Monitor sends a "template" email (via SMTP) to Clickatell's SMS gateway. This template email contains all the required SMS alert details including the SMS text message and the recipient's number. Clickatell then converts this email to SMS and sends it to the intended recipient. For more information, visit http://www.Clickatell.com/brochure/products/api_smtp.php.



Screenshot 110 - Clickatell Email2SMS Service configuration dialog

Requirements

No specific hardware is required for this SMS messaging method. The only true requirements are:

1. You must be subscribed to the Clickatell SMS gateway service. This service costs about 4 euro cents per message. To subscribe visit:
http://www.Clickatell.com/central/campaigns/redir.php?cid=870

2. The SMTP server configured in the properties of the Clickatell Email2SMS service must be able to send emails over the Internet.

GFI Network Server Monitor cannot send SMS alerts through Clickatell Email2SMS Service if no Internet connection is available or when your Internet connection is down.

Configuring the Clickatell Email2SMS Service

To configure the Clickatell Email2SMS Service:

1. Right Click on the 'Alerting Options' node and select 'Properties'.

2. Click on the 'SMS' tab and from the SMS System dropdown, select 'Clickatell Email2SMS Service'.

3. Double click on the property which you want to configure (e.g., SMTP server) and specify the relative parameters in the Edit Property dialog.

When configuring properties, always specify the details supplied to you by Clickatell. If configuration parameters are not available, ask Clickatell to provide you with the required information.

The Clickatell Email2SMS Service requires the following parameters:

- SMTP server – Specify the name of the SMTP server through which GFI Network Server Monitor will send the email to the SMS gateway.
- SMTP port – Specify the SMTP port through which the transmission will take place. By default this parameter is set to 25 (i.e., default SMTP port)
- From – Specify the account from where the email will be sent. For example you can specify the email address used by GFI Network Server Monitor for generic alerts.
- To – Specify the email address of the Clickatell SMS gateway (i.e., the address where GFI Network Server Monitor will send emails for conversion to SMS). This address is provided by Clickatell (i.e., by the SMS gateway provider). By default, this property is set to sms@messaging.Clickatell.com.

Leave this property as default, unless otherwise specified by Clickatell.

- CC* - (Optional parameter) Specify the email address where you wish to forward copies of the emails sent to the web based SMS gateway.
- Subject* - (Optional parameter) Specify the text which you want to include in the email's subject field.
- Body line 1 – Specify the API ID (e.g., api_id:124576). The API ID is an identification number supplied to you by Clickatell after you subscribe for the service. Format this parameter as follows: api_id:<API ID No>.

If you don't know your API ID, ask Clickatell to supply you with this information.

- Body line 2 - Specify your Clickatell SMS gateway user-name (e.g., user:JasonM). Format this parameter as follows: user:<user name>

If you don't know your user name, ask Clickatell to supply you with this information.

- Body line 3 - Specify your Clickatell SMS gateway password (e.g., password:abcde). Format this parameter as follows: password:<password text>

If you don't know your password, ask Clickatell to supply you with this information.

- Body line 4 – (Leave as default). This property contains the number of the SMS recipient (i.e. the number where the SMS will be sent). This number is automatically passed on by GFI Network Server Monitor through variable [smsnumber] which is substituted to text when the template email is generated. The contents of this property are formatted as follows: to:[smsnumber]
- Body line 5 - (Leave as default). This property contains the text which must be included in the SMS. These contents are automatically passed on by GFI Network Server Monitor through variable [smsmessage] which is substituted to text when the email is generated. The contents of this property are formatted as follows: text:[smsmessage].

4. In the 'Retries' entry box, specify the number of times that GFI Network Server Monitor will try to send the email to the web-based email to SMS provider should the first attempt fail.

5. Click on 'OK' to save your configuration settings.

7.8 Generic SMS service provider template

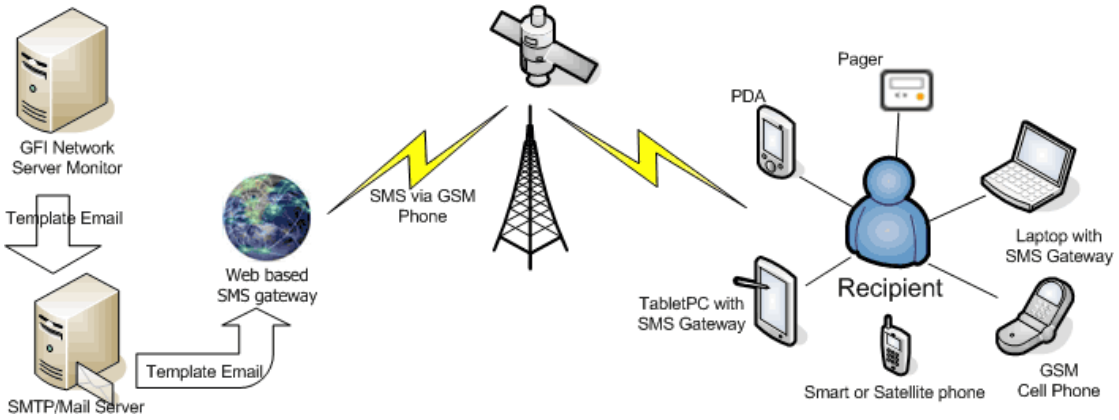
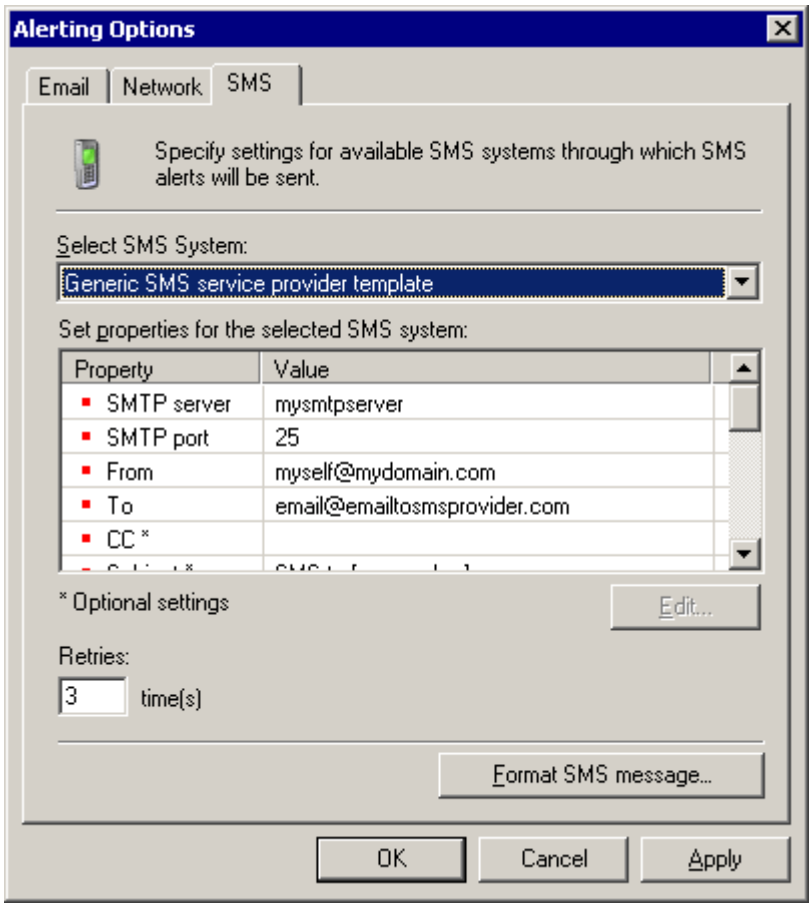


Figure 5 - SMS alert flow via a web-based Email to SMS service provider

GFI Network Server Monitor can relay SMS (text) alerts via a web-based SMS gateway.

Whenever an event triggers an SMS alert, GFI Network Server Monitor will send a "template" email (via SMTP) to a web-based SMS gateway. This template email contains all the required SMS alert details including the SMS text message and the recipient's number. The SMS gateway then converts this email to SMS and sends it to the intended recipient.

This template can be customized allowing you to use any provider which supports email to SMS services.



Screenshot 111 - Generic SMS service configuration dialog

Requirements

No specific hardware is required for this SMS messaging method. The only true requirements are:

1. You must be subscribed to an SMS gateway service.

2. The SMTP server configured in the properties of the Generic SMS service must be able to send emails over the internet.

GFI Network Server Monitor cannot send SMS alerts through the Generic SMS service if no Internet connection is available or when your Internet connection is down.

Configuring the Generic SMS service provider template

To configure the Generic SMS service:

1. Right click on the 'Alerting Options' node and select 'Properties'.

2. Click on the 'SMS' tab and from the SMS System dropdown, select 'Generic SMS service provider template.

3. Double click on the property which you want to configure (e.g., SMTP server) and specify the relative parameters in the Edit Property dialog.

When configuring properties, always specify the details supplied to you by your SMS gateway provider.

The Generic SMS service requires the following parameters:

- SMTP server – Specify the name of the SMTP server through which GFI Network Server Monitor will send the email to the SMS gateway.
- SMTP port – Specify the SMTP port through which the transmission will take place. By default this parameter is set to 25 (i.e., default SMTP port).
- From – Specify the account from where the email will be sent. You can specify the email address configured in GFI Network Server Monitor for generic alerts.
- To – Specify the email address of your SMS gateway provider (i.e., the address where GFI Network Server Monitor will send emails for conversion to SMS). This address is supplied by the SMS gateway provider and must be formatted as follows: <email>@<emailtosmsprovider.com>. E.g., sms@messaging.Clickatell.com.

If you don't know the email address of your SMS Gateway, ask your SMS gateway provider to provide this information.

- CC* - (Optional parameter) Specify the email address where you wish to forward copies of the emails sent to the SMS gateway.
- Subject* - (Optional parameter) Specify the text which you want to include in the email's subject field.
- Body line 1 – Specify the API ID which has been assigned to you by your SMS gateway provider. This parameter is required by the SMS gateway for authentication purposes. Format this parameter as follows: api_id:<API ID No>. E.g. api_id:124576.

If you don't know your API ID, ask your SMS gateway provider to supply you with this information.

- Body line 2 - Specify your SMS gateway user-name (e.g., user:JasonM). Format this entry as follows: user:<user name>.

If you don't know your SMS gateway user name, ask your SMS gateway provider to supply you with this information.

- Body line 3 - Specify your SMS gateway password (e.g., password:abcde). Format this entry as follows: password:<password text>.

If you don't know your SMS gateway password, ask your SMS gateway provider to provide this information.

- Body line 4 – (Leave as default). This property contains the number of the SMS recipient (i.e., the number where the SMS will be sent). This value is automatically passed on by GFI Network Server Monitor through variable [smsnumber] which is substituted to text when the email is generated. The contents of this property are formatted as follows: to:[smsnumber]
- Body line 5 - (Leave as default). This property contains the text which must be included in the SMS. These contents are automatically passed on by GFI Network Server Monitor through variable [smsmessage] which is substituted to text when the email is generated. The contents of this property are formatted as follows: **text:**[smsmessage].

4. In the 'Retries' entry box, specify the number of times that GFI Network Server Monitor will try to send the email to the web-based email to SMS provider should the first attempt fail.

5. Click on 'OK' to save your configuration settings.

7.9 NSM 5.x/6.0 SMS Server system

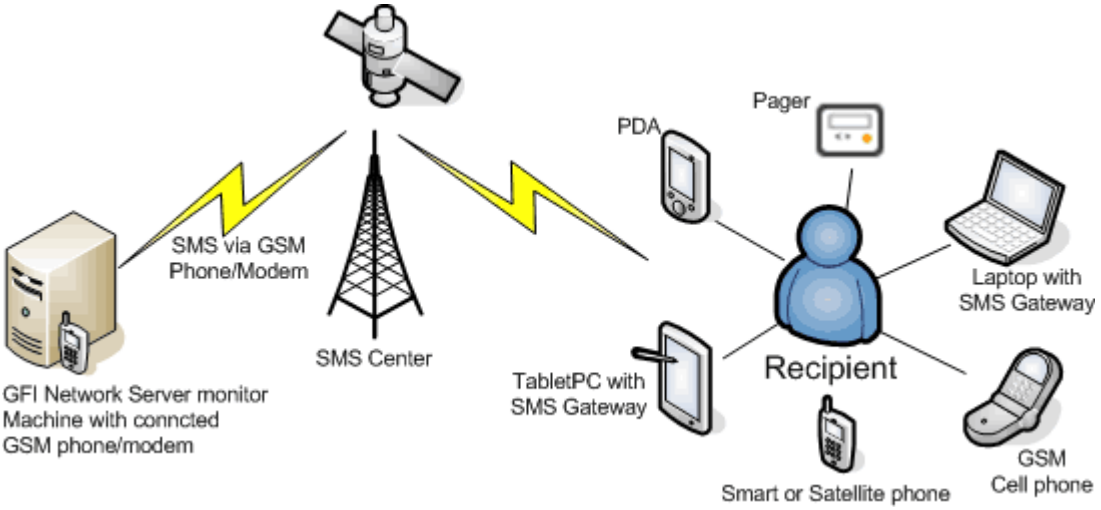


Figure 6 - SMS alert flow via the NSM 5.x/6.0 SMS server

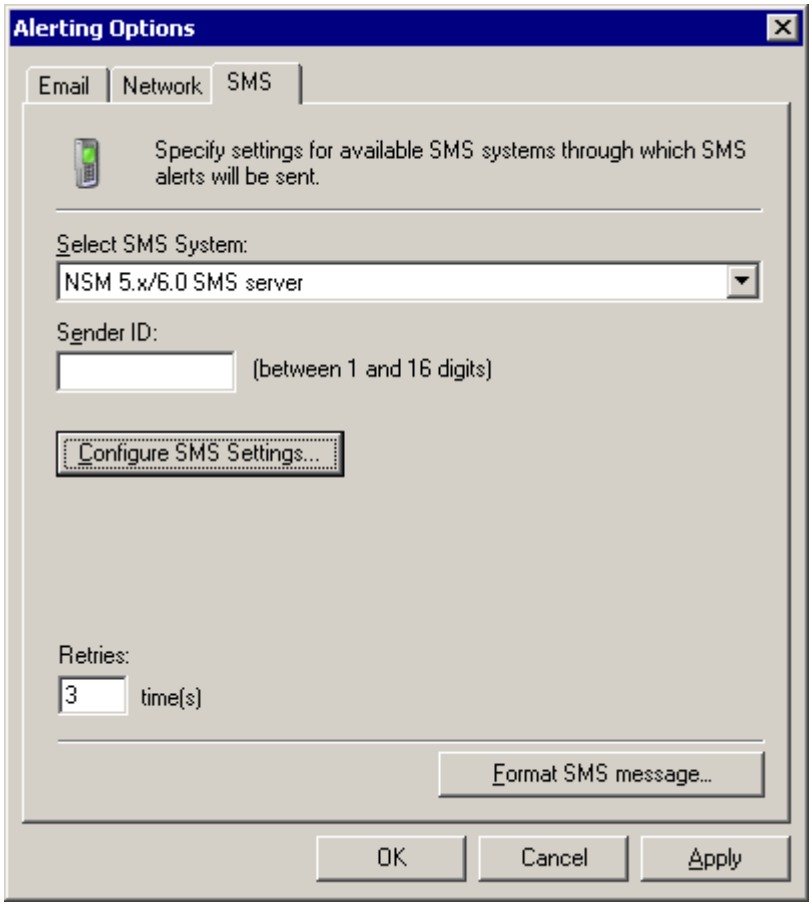
The NSM 5.x/6.0 SMS Server can send SMS (text) messages through a TAP/UCP compliant SMSC (Short Message Service Center)

The Sender ID is the number of the sending entity. Leave this empty if you want your ID to be withheld when sending a message.

Requirements

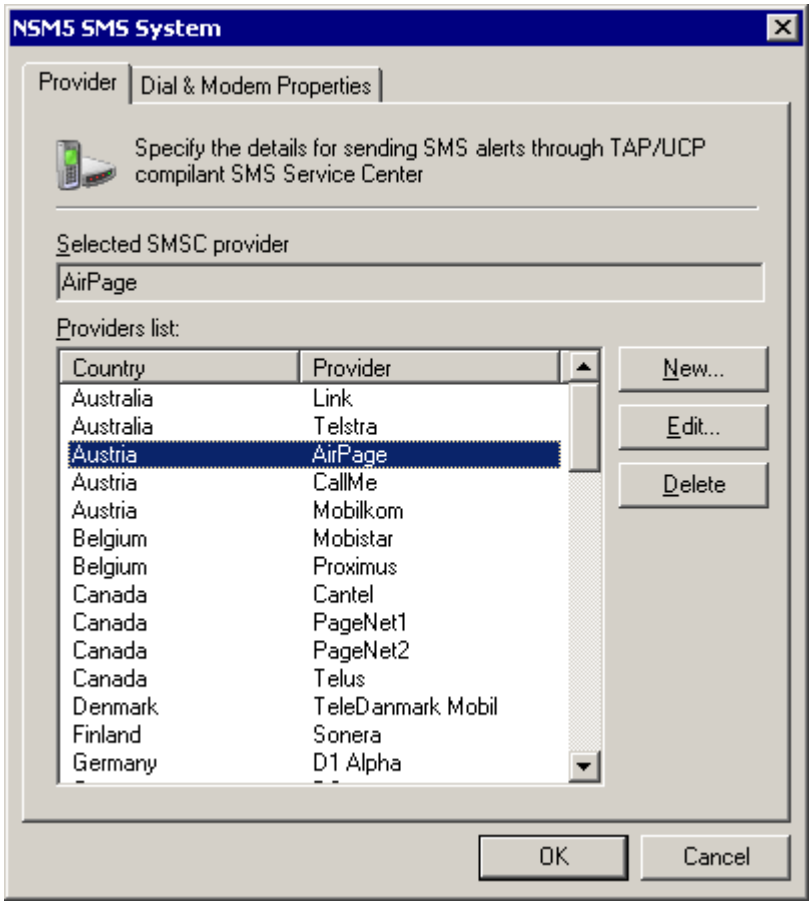
This NSM 5.x/6.0 SMS messaging method requires a normal Hayes-compatible modem connected to the server on which the GFI Network Monitor Engine is running. When a check fails, GFI Network Server Monitor uses the modem to dial in to the SMSC provider and deliver the actual SMS message(s); most countries have one or more SMSC service providers.

Configuring a TAP/UCP compliant SMS Service Center



Screenshot 112 - NSM 5 SMS Server configuration dialog

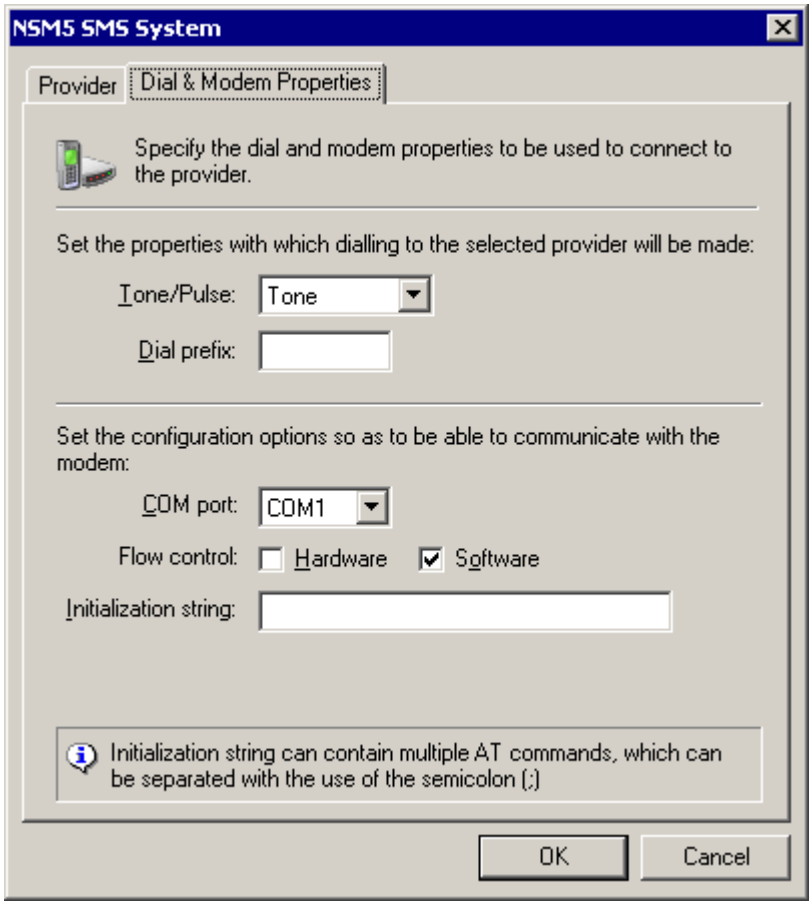
1. Right click on the 'Alerting Options' node and select 'Properties'.
2. Click on the 'SMS' tab and from the SMS System dropdown, select 'NSM 5.x/6.0 SMS Server'.
3. Click on the 'Configure SMS Settings' button.



Screenshot 113 - Providers tab

4. Choose your SMSC service provider from the available list of providers.

To add unlisted providers, refer to the 'Adding new SMSC providers' section in this chapter.


NSM5 SMS System
Provider
Dial & Modem Properties
Specify the dial and modem properties to be used to connect to the provider.
Set the properties with which dialling to the selected provider will be made:
Tone/Pulse:
Tone
Dial prefix:
Set the configuration options so as to be able to communicate with the modem:
COM port:
COM1
Flow control:
Hardware
Software
Initialization string:
Initialization string can contain multiple AT commands, which can be separated with the use of the semicolon (;)
OK
Cancel

Screenshot 114 - Dial & Modem properties tab

5. Click on the 'Dial and Modem Properties' tab and specify the following parameters:

- Tone/Pulse – Select the type of dialing that your modem will use (i.e., tone or pulse).
- Dial prefix – Specify any additional numbers that need to be dialed before the dial-string.

The dial-string is the number of the selected provider and can only be modified by editing the SMSC provider's details. For further information, please refer to the 'Changing SMSC providers details' section in this chapter.

- *COM* Port - Select the com port where the modem is connected.
- Flow Control – (Leave as default).
- Initialization *String* - If required, specify any AT Commands that you wish to send to your modem.

The initialization string is a set of modem AT commands combined into one string (e.g., AT &F &C1 &D2). For a complete list of AT commands visit http://esvc001164.wic013u.server-web.com/modems/modemstrings.htm

6. Click on 'OK' to close the configuration dialog.

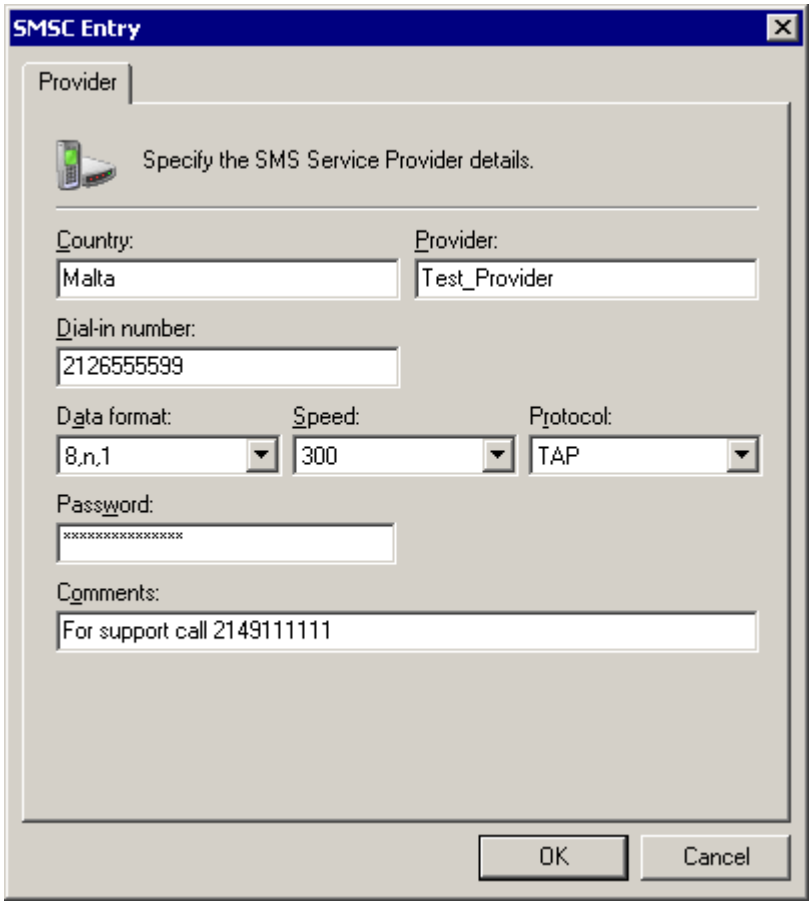
7. In the 'Retries' entry box, specify the number of redial attempts required before the connection is timed out.

8. Click on 'OK' to save your configuration settings.

Add new SMSC providers

GFI Network Server Monitor includes an extensive list of SMS service providers. However, it maybe necessary to add new providers from time to time. To add a new provider:

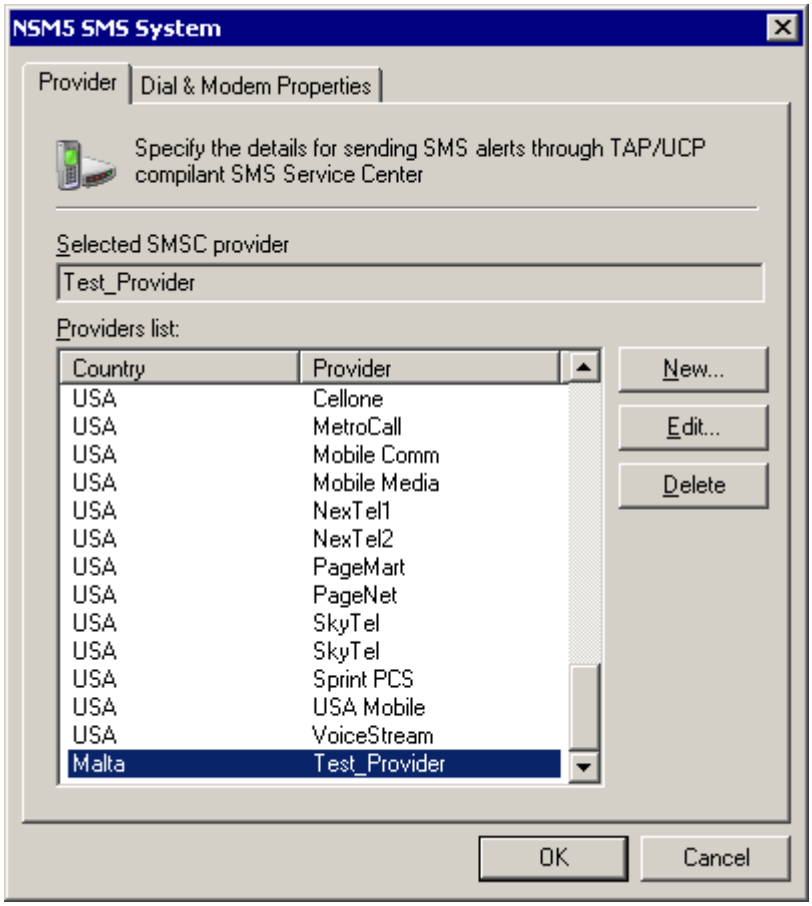
1. Right click on the ‘Alerting Options’ node and select ‘Properties’.
2. Click on the ‘SMS’ tab and from the SMS System dropdown, choose ‘NSM 5.x/6.0 SMS Server’.
3. Click on the ‘Configure SMS Settings’ button.



Screenshot 115 - SMSC Provider Setup Screen

4. Click on ‘New’ and specify the following parameters:
   - » Country - Specify the country of the provider.
   - » Provider - Specify the provider name.
   - » Dial-in number - Specify the number that the modem must dial to connect to the provider.
   - » Data format - Specify the data format to be used. Obtain this information from your service provider.
   - » Speed - Specify the speed at which the data must be sent. Obtain this value from your SMS service provider.
   - » Protocol - Choose between TAP (Telecator Alphanumeric Protocol) and UCP (Universal Computer Protocol). Although TAP is the most commonly used protocol, you should ask your SMS service provider for this information.
   - » Password - You can specify a password to use for authentication before connecting to the provider.
   - » Comments – Add any comment related to the provider (e.g., For support, call provider on 22211164)
5. Click on ‘OK’ to add the service provider to the list.

Changing SMSC providers details



Screenshot 116 - SMSC providers list

This section is only applicable for advanced users. We cannot guarantee that GFI Network Server Monitor will work with any SMS provider. Ensure that you obtain the correct information from your SMS service provider first. To change the provider's details:

1. Right click on the 'Alerting Options' node and select 'Properties'.
2. Click on the 'SMS' tab and from the SMS System dropdown, select 'NSM 5.x/6.0 SMS Server'.
3. Click on the 'Configure SMS Settings' button.
3. Choose the SMSC service provider from the list. Click on 'Edit' and make the required changes.
4. Click on 'OK' to save the changes.

7.9.1 Additional notes

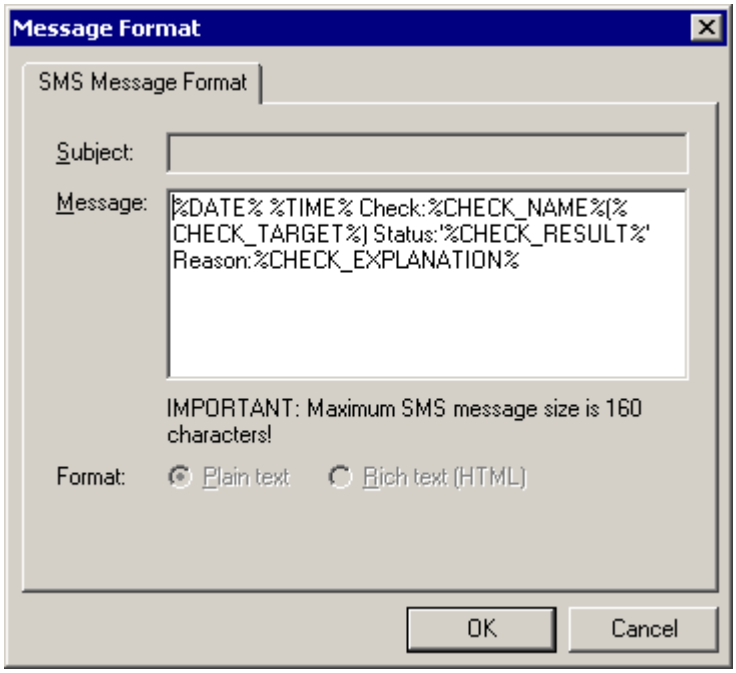
SMSC providers require the connection speed. Therefore configure this in the provider details.

The number format of a recipient depends on the provider (when using SMSC). This requires an amount of trial and error to find the right format; for example, if you live in the UK (international dialing code: +44), you should try:

- 12345678
- 4412345678
- 004412345678

Format SMS/pager message

1. Right Click on the 'Alerting Options' node and select 'Properties'.
2. Click on the 'SMS' tab and then click on 'FORMAT SMS MESSAGE'.



Screenshot 117 - SMS/Pager Message Format Window

3. Make the necessary changes to the SMS message and click on 'OK' to accept changes. For more information on variables and message templates formatting, refer to the 'Message Template' section in this chapter.

7.10 Message templates

Alert messages templates can be customized by clicking on the 'Format Message' button present in the Email, Network, and SMS/Pager pages of the NSM Global Alerting options. Message templates can be built up using text and variables. Variables are substituted each time a message is sent out and must be enclosed within "%" (e.g. %DATE%) when specified in message templates. The following are variables that can be included in message templates:

- %DATE% - date in mm/dd/yyyy format.
- %TIME% - time in hh:mm:ss format.
- %CHECK_NAME% - the display name of the check as seen in the configuration.
- %CHECK_FOLDER% - the name of the folder in which the specific check is located.
- %CHECK_TARGET% - the check's target computer name/IP; can be either the one set in the check or the one inherited from the parent folder.

- %CHECK_RESULT% - the result of the monitoring of the check represented as a string.
- %CHECK_EXPLANATION% - the explanation returned with the last known status of the check.
- %CHECK_DESCRIPTION% - A description of the function carried out by the check.
- %PRODUCTNAME% - the (short) product name of the product (i.e. GFI N. S. M. 6.0).

Example of a message template:

Message from GFI Network Server Monitor, <% DATE %> <%TIME %>:

Item: <% CHECK_TARGET %>

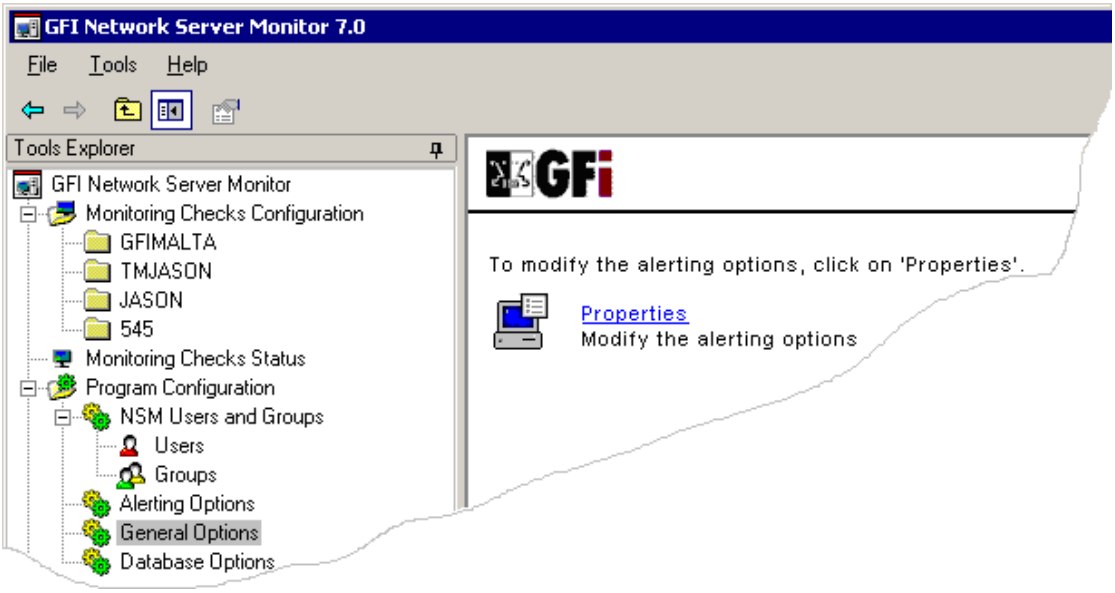
Result: <% CHECK_RESULT %>

Explanation: <% CHECK_EXPLANATION %> Message from GFI Network Server Monitor, <% DATE %> <%TIME %>

Using new lines in SMS/Pager Message Templates is NOT recommended. Most GSM phones don't know how to handle new lines and will display bad characters.

8 General options

8.1 Introduction



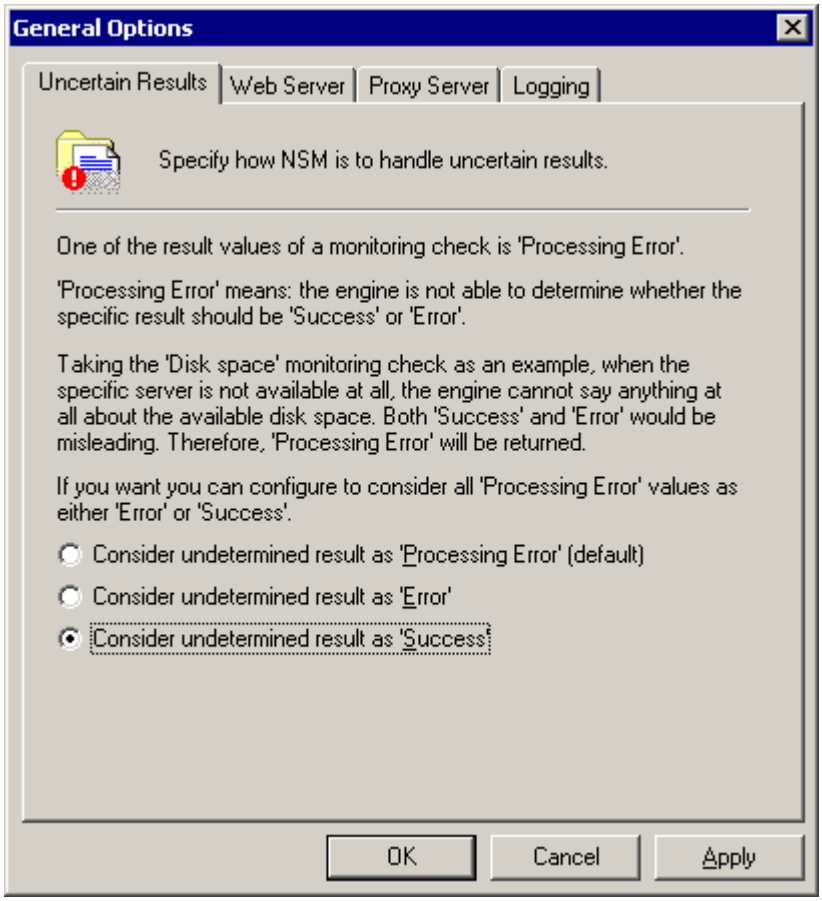
Screenshot 118 - 'General Options' node

From the 'General Options' node you can:

- Specify how GFI Network Server Monitor will handle uncertain results.
- Configure GFI Network Server Monitor built in Web server.
- Specify which proxy server will be used for Internet Protocol based checks.
- Enable the event logging activity.

8.2 Uncertain Results settings

An uncertain result occurs when the result of a check cannot be determined as successful or failed by the GFI Network Server Monitor engine because of the condition encountered (e.g. If the target computer on which a monitor function checks Disk Space can no longer be accessed, then the check status is set to uncertain, because GFI Network Server Monitor engine can no longer determine the disk space).


General Options
Uncertain Results
Web Server
Proxy Server
Logging
Specify how NSM is to handle uncertain results.
One of the result values of a monitoring check is 'Processing Error'.
'Processing Error' means: the engine is not able to determine whether the specific result should be 'Success' or 'Error'.
Taking the 'Disk space' monitoring check as an example, when the specific server is not available at all, the engine cannot say anything at all about the available disk space. Both 'Success' and 'Error' would be misleading. Therefore, 'Processing Error' will be returned.
If you want you can configure to consider all 'Processing Error' values as either 'Error' or 'Success'.
Consider undetermined result as 'Processing Error' (default)
Consider undetermined result as 'Error'
Consider undetermined result as 'Success'
OK
Cancel
Apply

Screenshot 119 - Uncertain Results setup

GFI Network Server Monitor can be configured to convert uncertain results to a definite state i.e. Success or Error. To specify how GFI Network Server Monitor will handle uncertain results:

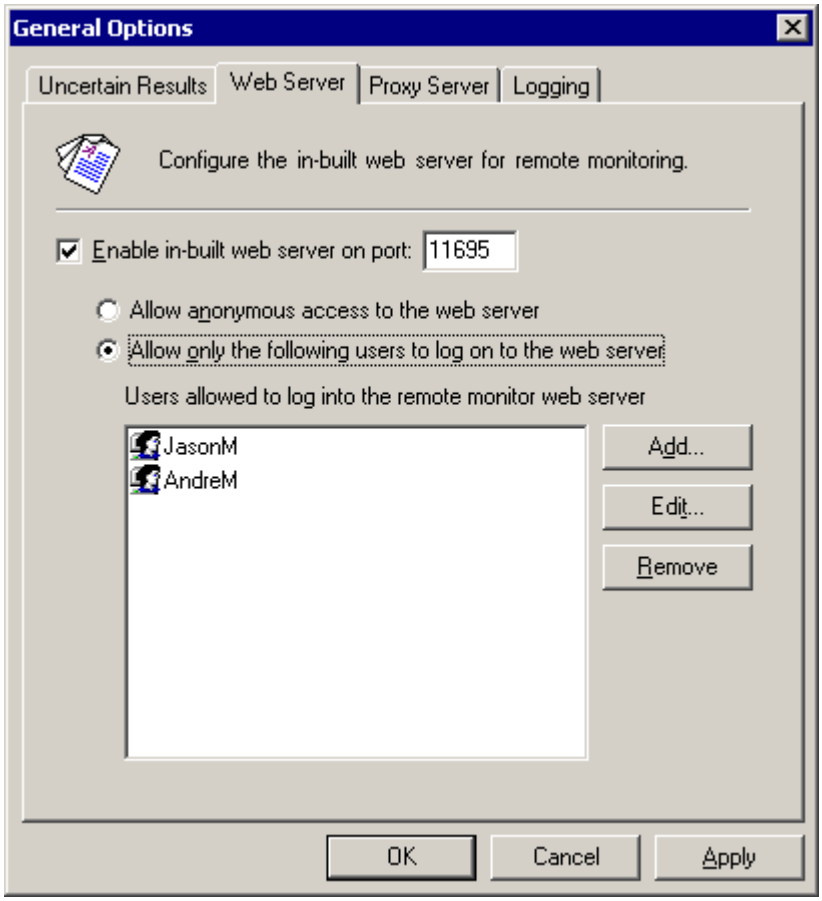
1. Right Click on the ‘General Options’ node and select ‘Properties’. By default the properties dialog will open in the Uncertain Results (tab) options.

2. Determine uncertain results by:

- Enabling ‘If result cannot be determined, consider result as ‘Uncertain’ (default)’ to leave uncertain results unhandled.
- Enabling ‘If result cannot be determined, consider result as ‘Error’’ to handle uncertain results as failed.
- Enabling ‘If result cannot be determined, consider result as ‘Success’ to handle uncertain results succeeded. In this case, the same conditions specified on the successful execution of a check will apply.

8.3 Web Server settings

You can use the GFI Network Server Monitor built in web server to remotely view the status of your network.



Screenshot 120 - built in Web Server settings

To configure the built in web server:

1. Right Click on the 'General Options' node, select 'Properties' and click on the 'Web Server' tab.

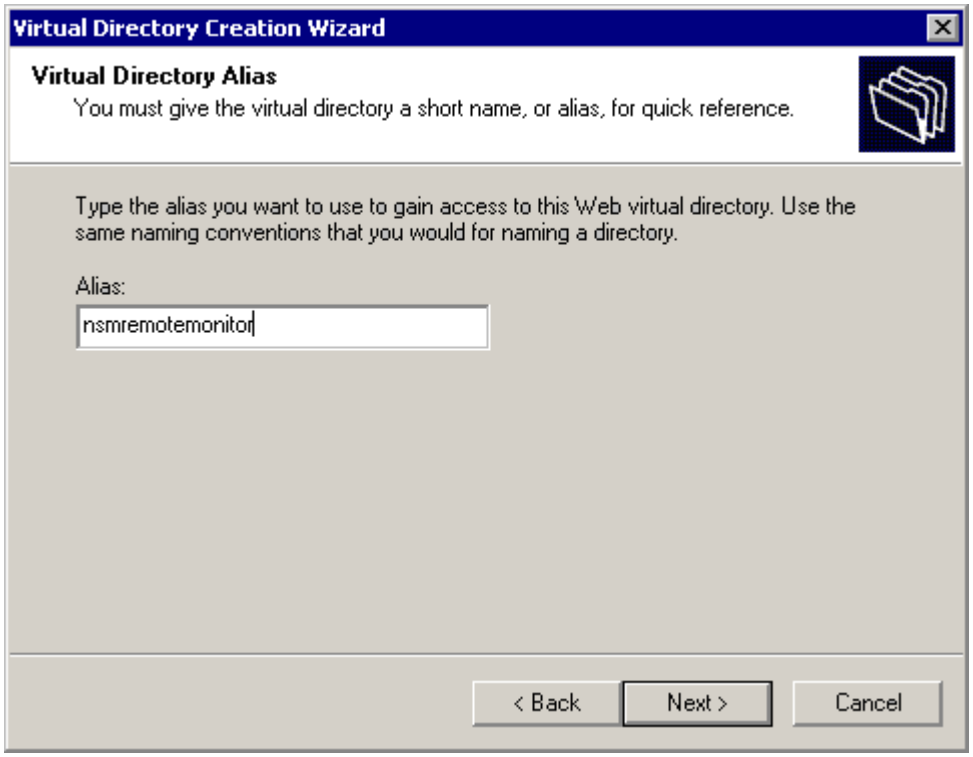
2. Configure the following parameters:

- 'Enable in-built web server on port….' – Enable this flag and specify the port which the built in web server will listen on (by default set to 11695).
- 'Allow anonymous access to the web server' – Enable this flag to indicate that no authentication is required on the web server.
- 'Allow only the following users to log on to the web server' – Enable this flag to grant web server access only to the specified users.
- To specify users that have access to the web server, click on 'Add'. Then, specify the user's authentication details (User name and Password) and click on 'OK'.

8.3.1 Configuring IIS as the web server

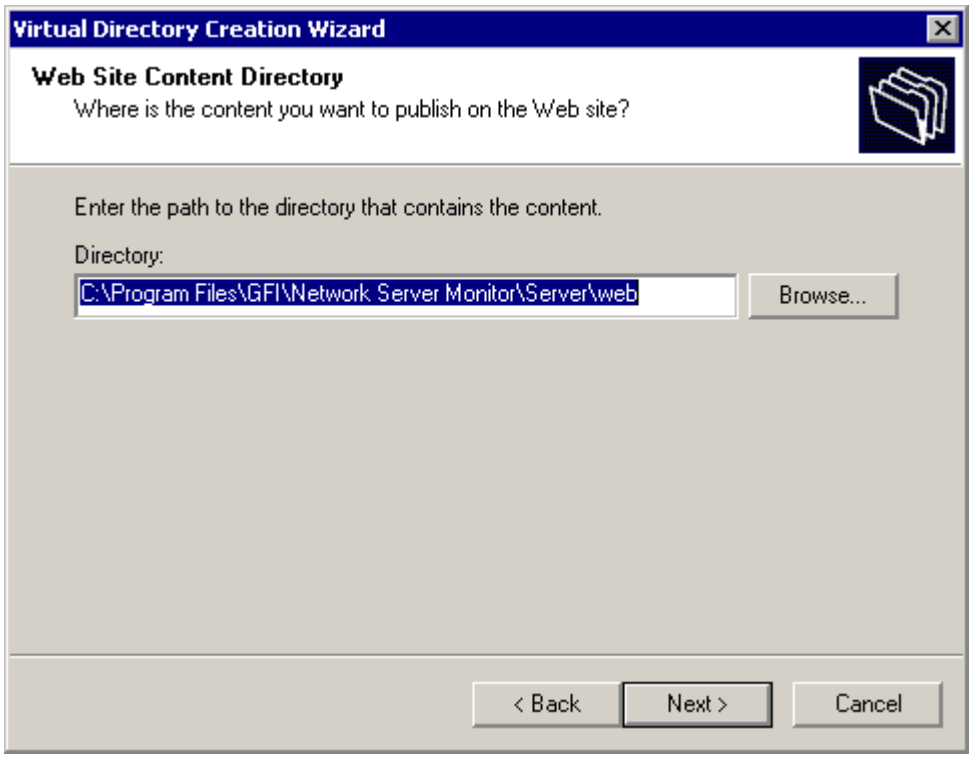
Using IIS as the web server gives you more advanced authentication features and the possibility to secure the connection via SSL. The integration with IIS is very straightforward. GFI Network Server Monitor updates an XML file, from which the 2 views are rendered. These files are stored in the GFI Network Server Monitor\Server\web folder. You need to create a virtual directory in IIS, which points to the GFI Network Server Monitor\Server\Web folder. To do this:

1. Start up Internet Services Manager, right click on the 'Web Site' node, and from the popup menu select 'New – Virtual Directory'.


Virtual Directory Creation Wizard
Virtual Directory Alias
You must give the virtual directory a short name, or alias, for quick reference.
Type the alias you want to use to gain access to this Web virtual directory. Use the same naming conventions that you would for naming a directory.
Alias:
nsmremotemonitor
< Back
Next >
Cancel

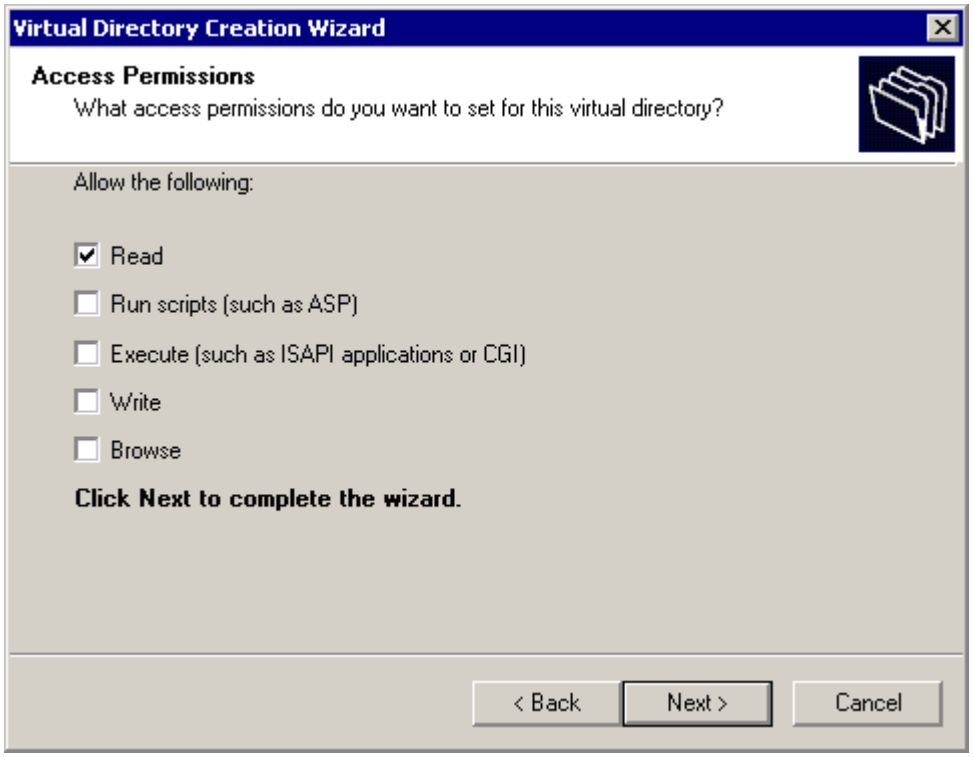
Screenshot 121 - Specifying an alias for the virtual directory

2. This will start the Virtual Directory Creation Wizard. Click on 'Next' to continue. Now you need to enter an alias for the virtual directory. In this case it is nsmremotemonitor, but you can enter whatever name you like, as long as it follows the folder naming conventions used in Microsoft Windows.


Virtual Directory Creation Wizard
Web Site Content Directory
Where is the content you want to publish on the Web site?
Enter the path to the directory that contains the content.
Directory:
C:\Program Files\GFI\Network Server Monitor\Server\web
Browse...
< Back
Next >
Cancel

Screenshot 122- Pointing to the GFI NSM web folder

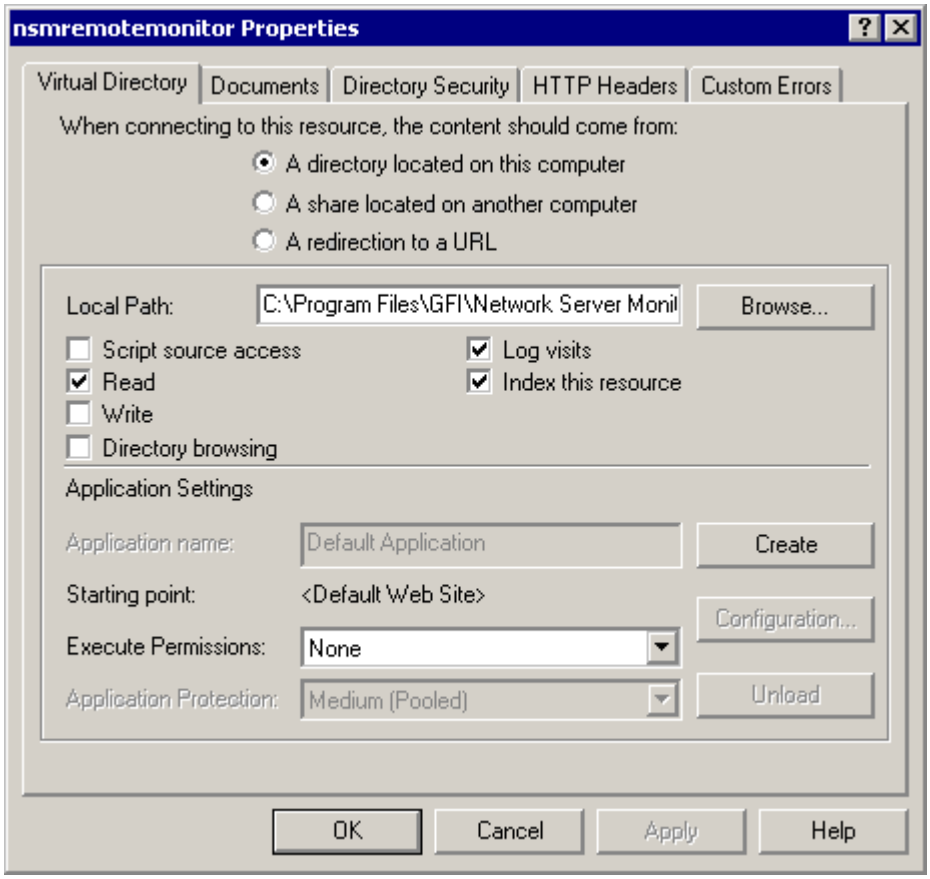
3. Now enter the path where the content is located. Select 'Browse', and select the 'server\web' folder in the GFI Network Server Monitor installation path.



Screenshot 123 - Setting permissions

4. Next we need to set the access permissions. Mark 'Read' only. Do not mark any of the other check boxes. Click on 'Next' to finish the Virtual Directory Creation Wizard.

5. Right-click on the newly created virtual directory, located under the web root of your web site server and select 'Properties'.



Screenshot 124 - Setting Virtual Directory properties

6. In the Virtual Directory tab of the properties dialog, mark the 'Read', the 'Log Visits' and the 'Index this resource' check boxes.

7. Click on ‘OK’ to close the properties dialog. The Virtual Directory has been set-up and you can now test access to it.

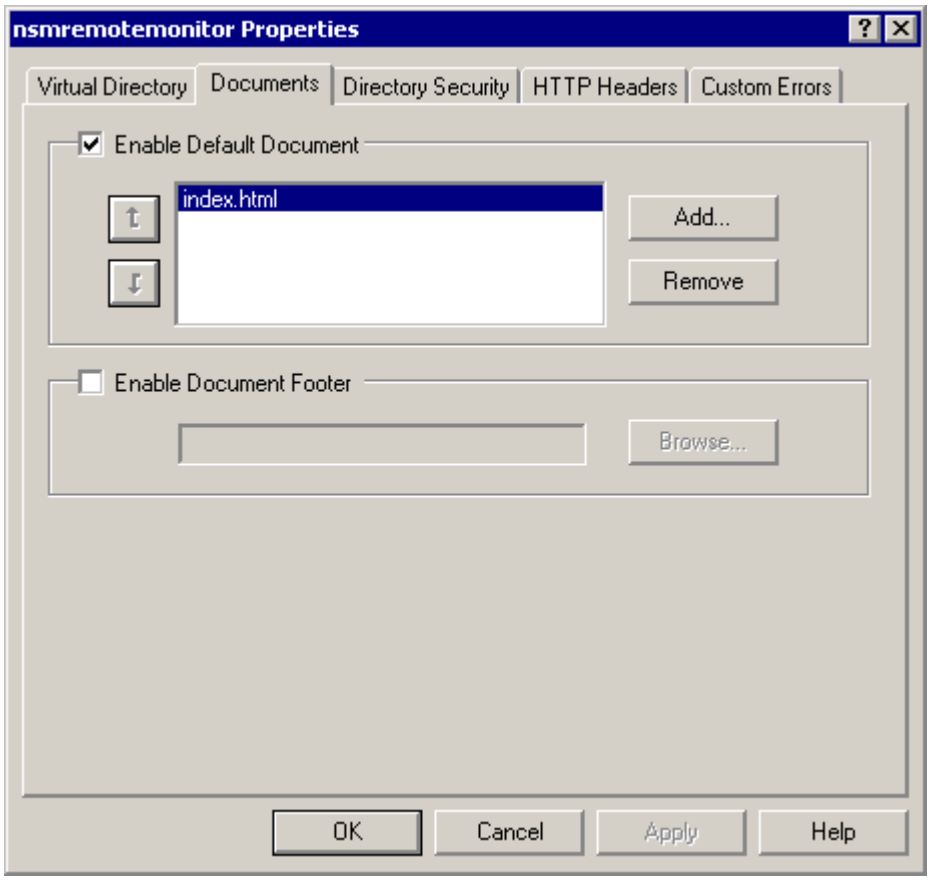
8.3.2 Securing the Remote Monitor

It is important to set up proper authentication and security for this web server and virtual directory. There are three ways to secure the Remote Monitor. These are Basic Authentication, Digest and Integrated Windows Authentication. Integrated Windows Authentication is the preferred choice in an Active Directory environment, because it makes the authentication process seamless, since initially it does not prompt users for their user name or password information. It uses the current Windows user information on the client computer for authentication, instead. If you are installing GFI Network Server Monitor on a DMZ, you must use Basic authentication.

The following steps show how to secure access to the Web based remote monitor.

1. Open up Internet Services Manager. Right click on the Network Server Monitor Remote Monitor virtual directory under your server web site and select ‘Properties’.

2. Under the Virtual Directory tab make sure to deselect Directory Browsing.

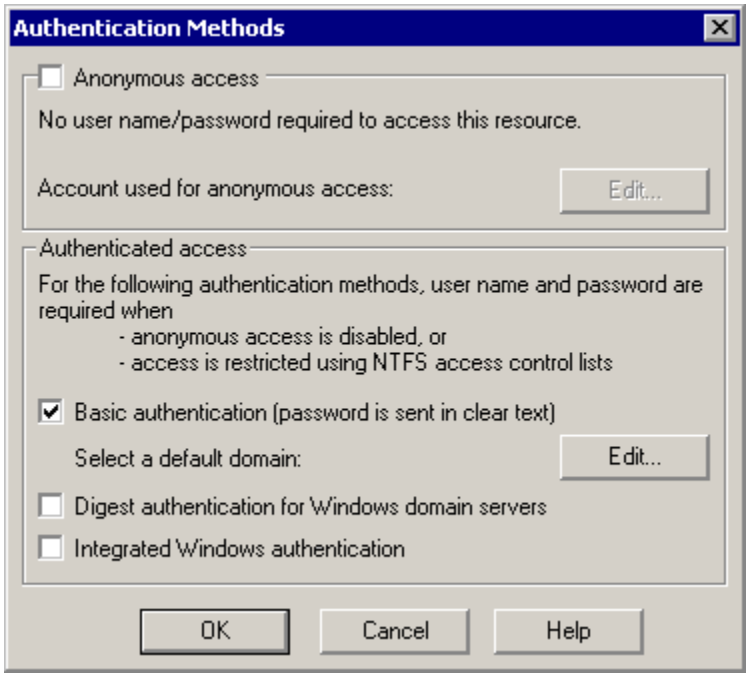


Screenshot 125 - Specify default document

3. Select the Documents tab and remove all the default documents. Add the following default document ‘index.html’.

4. Select the Directory Security tab and click on ‘Edit’ for the Anonymous access and authentication control group.

5. Select Integrated Windows authentication (recommended if installed on the internal network) OR Basic Authentication check box (if installed in the DMZ). Ensure Anonymous access is deselected.

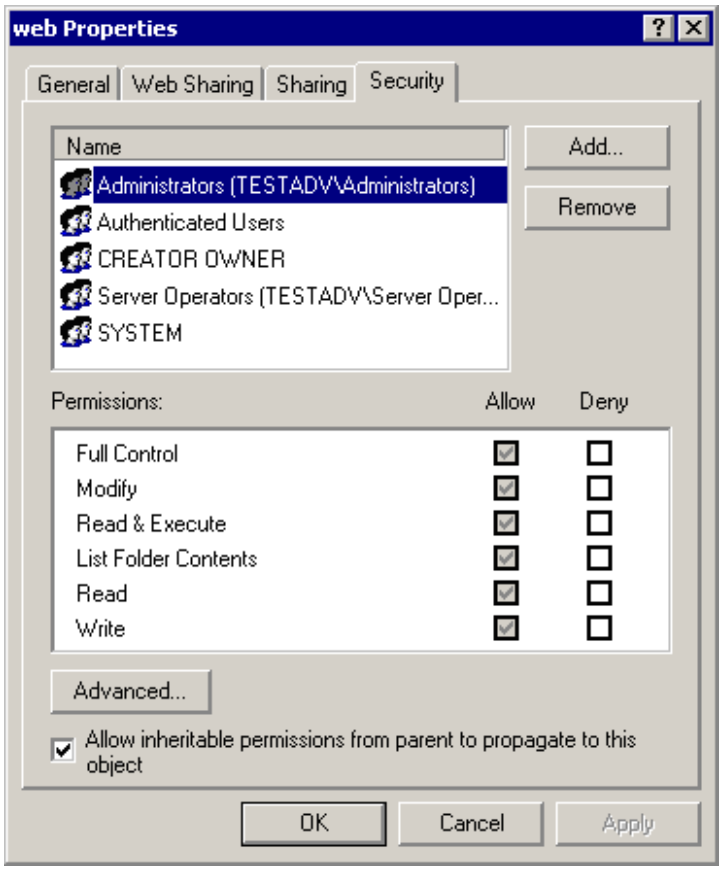

Authentication Methods
Anonymous access
No user name/password required to access this resource.
Account used for anonymous access:
Edit...
Authenticated access
For the following authentication methods, user name and password are required when
- anonymous access is disabled, or
- access is restricted using NTFS access control lists
Basic authentication (password is sent in clear text)
Select a default domain:
Edit...
Digest authentication for Windows domain servers
Integrated Windows authentication
OK
Cancel
Help

Screenshot 126 - Select authentication method

If Integrated Windows authentication is used, then authentication will occur against Active Directory. This means you do not need to configure additional users. If you use Basic Authentication, authentication will occur against the local user database on the computer. In this case you must create user names and passwords on that local computer. For more information on securing IIS, please review the IIS documentation.

Be sure not to allow anonymous access!

6. Restrict the access to the pages by using NTFS permissions. Open up Explorer and navigate to the web folder in the GFI Network Server Monitor installation path. Right click on the ‘web’ sub folder, select ‘Properties’ and then the ‘Security' tab.

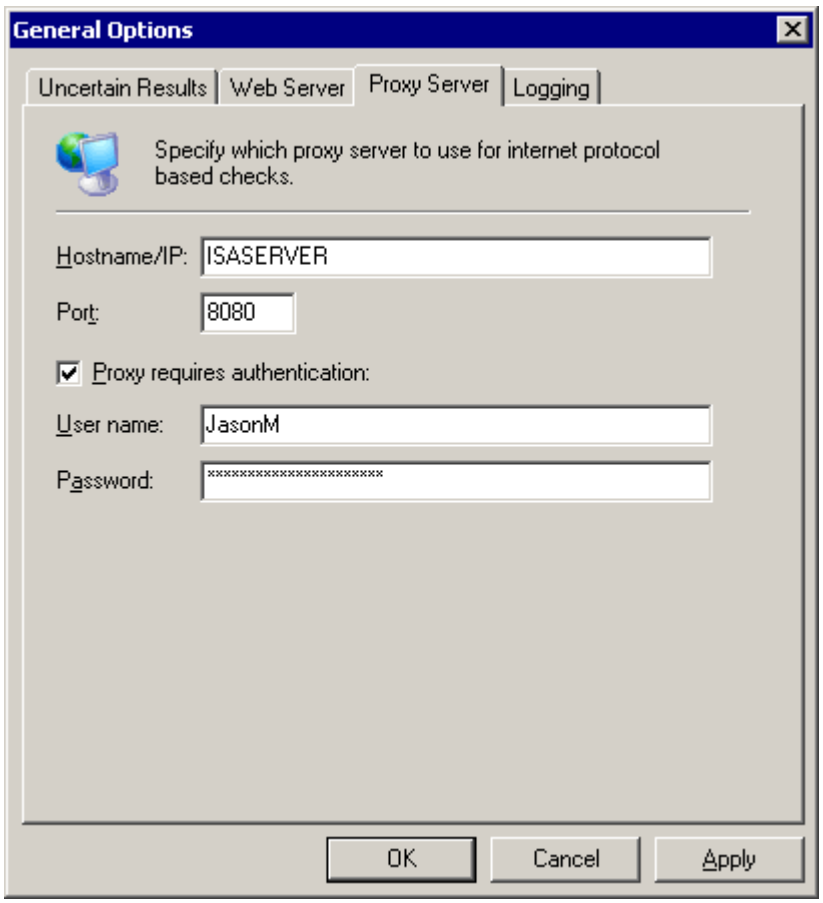


Screenshot 127 - Setting permissions

7. Add / remove the users / groups you want to grant access to the Remote Monitor. To grant access only to users forming part of the administrators group, you would set the security tab. Click on 'OK' to finally secure the remote monitor.

8.4 Proxy Server settings

The proxy server settings define which server will be used for Internet protocol checks.



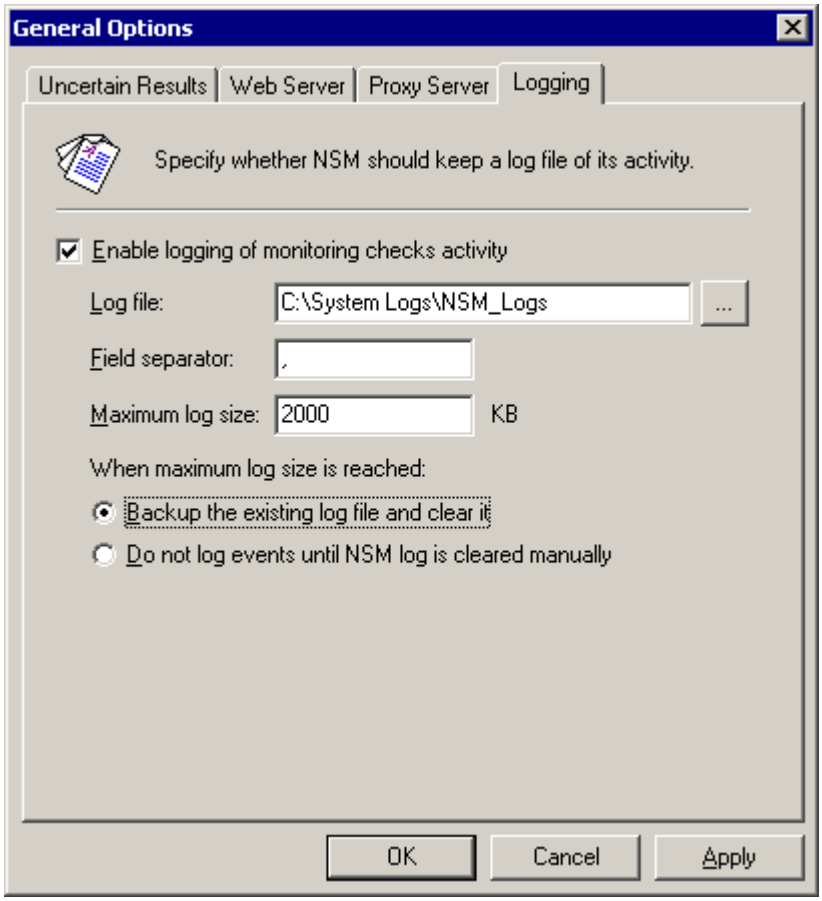
Screenshot 128 - Proxy Server Setup Window

To configure proxy server parameters:

1. Right Click on the 'General Options' node and select Properties.
2. Click on the Proxy Server Tab and define the following parameters:
   - » Hostname/IP Address – Specify the proxy server name (e.g. ISASERVER) or IP address.
   - » Port – Specify the port on which the proxy server will listen (default = 8080).
   - » Proxy requires authentication – Enable this flag to indicate that the specified proxy server requires authentication details.
   - » User name / Password – Specify the logon detail to be passed to the specified proxy server for authentication.

8.5 Log file settings

GFI Network Server Monitor can log monitoring checks activity into a text file for future reference. Since the log file is in plain text, you can import its contents to other applications for further processing.



Screenshot 129 - Log file setup Window

To configure the logging parameters:

1. Right Click on the 'General Options' node and select 'Properties'.
2. Click on the 'Logging' tab and define the following parameters:

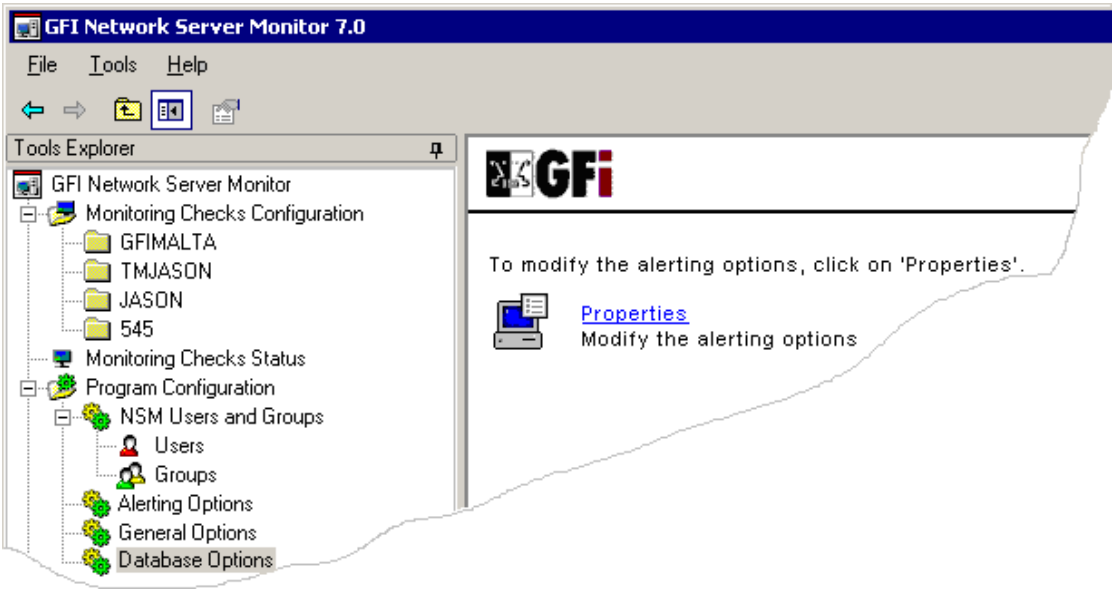
- 'Enable Logging of monitoring checks activity' – Enable this flag to start logging all check activity to a specified text file.
- Log file – Specify the full path to the log file.
- Field separator – Specify the character that will be used to separate the fields in the log file (e.g. using the comma (,) would enable you to import the file to excel as CSV).
- Maximum log size – Specify the maximum log file size (in KB) required (e.g. if a 1 MB log file limit is required, specify 1000KB).
- 'Backup the existing log file and clear it' – Enable this option to automatically make a copy of the log file and clear the contents of the original log file whenever the specified file size limit is reached.

In such cases, the backup file name to be used would be 'LOG####.TXT' where #### is the next available number, depending on the number backup files that already exist (e.g. if LOG0002.TXT exist, the next backup file number will be LOG0003.TXT).

- *'Do not log events until event log is cleared manually'* – Enable this option to stop logging check activity whenever the maximum specified log file size is reached.

9 Database maintenance options

9.1 Introduction



Screenshot 130 - Database Options

Through the 'Database Maintenance Options' node, you can select and configure the database backend to use for the storing of monitoring results data. You can choose between MS Access and MS SQL Server as a database backend. In the case of SQL Server, you can also specify the type of authentication to use when logging onto the database (SQL Server authentication or Windows authentication).

Windows NT authentication mode allows you to log onto the SQL Server database using your Windows account details. The SQL Server authentication mode allows you to log on to the database using the SQL Server account details (i.e., the credentials stored in ACL tables of SQL Server).

For more information on the authentication modes supported by SQL Servers visit

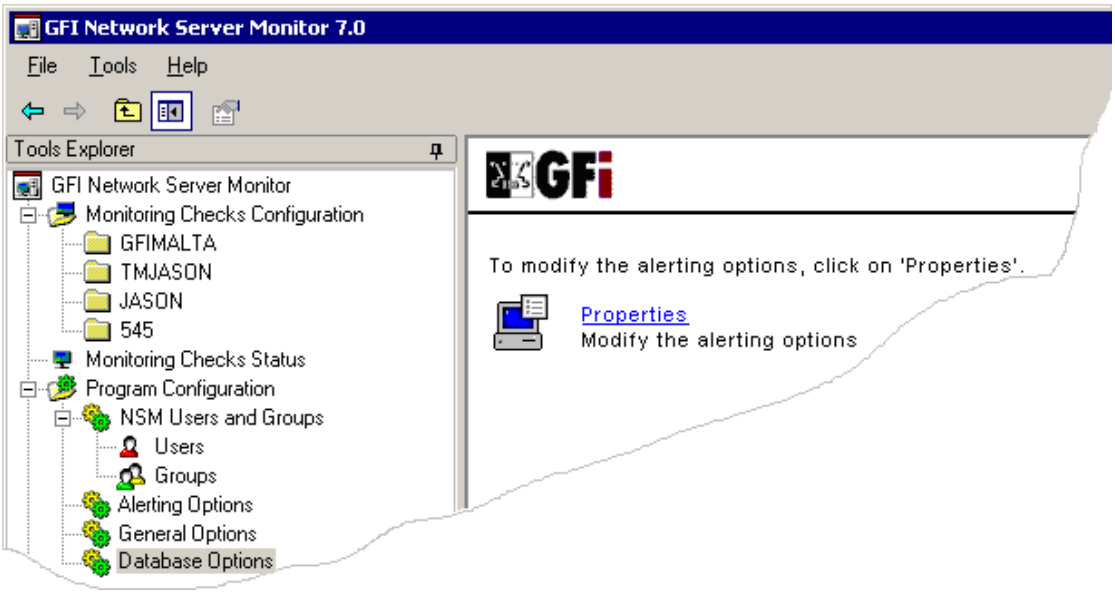
http://www.windowsecurity.com/articles/SQL_Server_2000_Authentication.html

Support for SQL Server database backend is only available during evaluation and in the Consultants/Enterprise editions of GFI Network Server Monitor.

9.2 Configuring the database backend

To configure the database backend used by GFI Network Server Monitor, right click on the 'Database Maintenance Options' node and select 'Properties'.

9.2.1 MS Access database backend

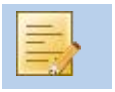


Screenshot 131 - Ms Access backend properties dialog

To use an Ms Access database backend:

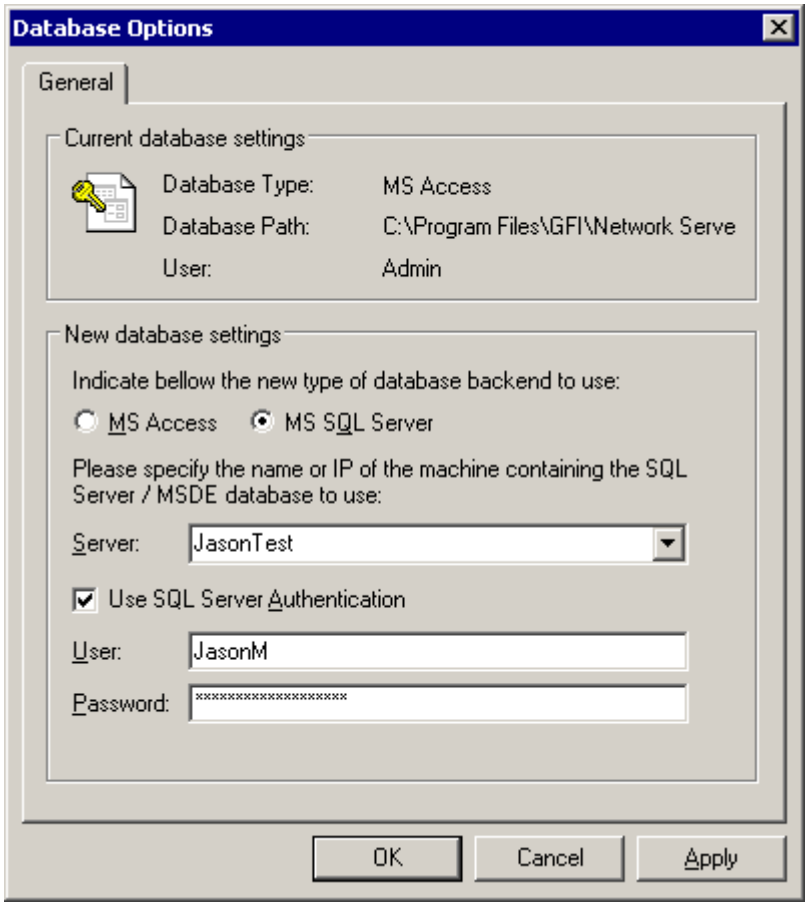
1. Select the 'MS Access' option and specify the full path (including file name) of your MS Access database backend.

2. Click on 'OK' to save your configuration settings.



If the specified database file does not exist, it will be created for you.

9.2.2 MSDE/MS SQL Server database backend



Screenshot 132 - MSDE/MS SQL Server backend properties dialog

To use an MSDE/MS SQL Server database backend:

1. Select the 'MS SQL Server' option and specify the name/IP of your SQL Server.

2. Specify the authentication mode to be used when logging on to the SQL Server. GFI Network Server Monitor supports both Windows NT and SQL authentication modes. To use SQL authentication, select the 'Use SQL Server Authentication' option and specify the SQL Server access credentials. For Windows NT authentication mode, select the 'Windows NT authentication' option.

If the specified server and credentials are correct, GFI Network Server Monitor will log into the SQL Server and create the necessary database tables. If the database tables already exist, it will re-use them.

3. Click on 'OK' to save your configuration settings.

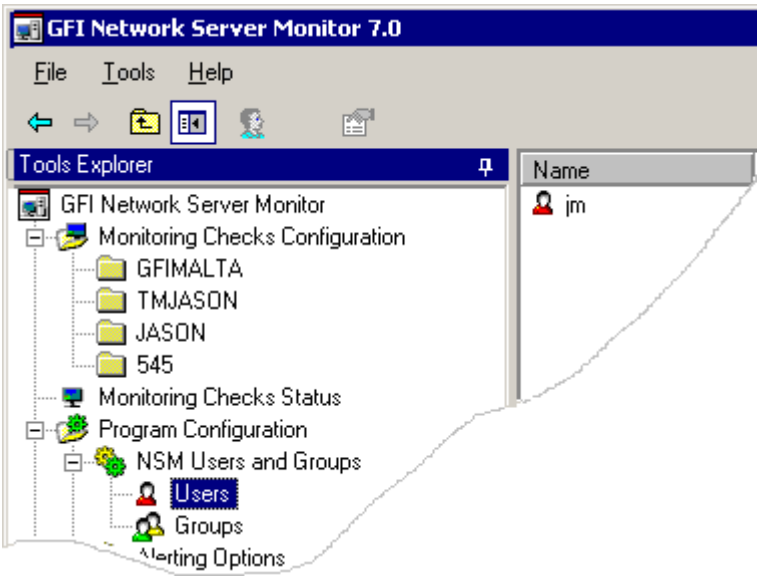
10 Users and Groups

10.1 Introduction

GFI Network Server Monitor checks refer to the user's properties to gain alert details (e.g., email address), rather than directly to an email or a number. This is in order to avoid having to change all the checks if a particular email or number of a user changes. You can configure user name, email address, mobile number, pager number and the computer name(s) from where network messages should be sent, from the user properties.

You can also define the working hours of a user and decide what alert (if any) is to be sent depending on the time that the important event occurred i.e. during or outside of working hours.

You can create a group of users to notify more than 1 person and avoid having to specify multiple users for each check you create. This makes it much easier to change the users to notify afterwards since you just need to change the group membership.



Screenshot 133- Users and Groups folders

10.2 Users

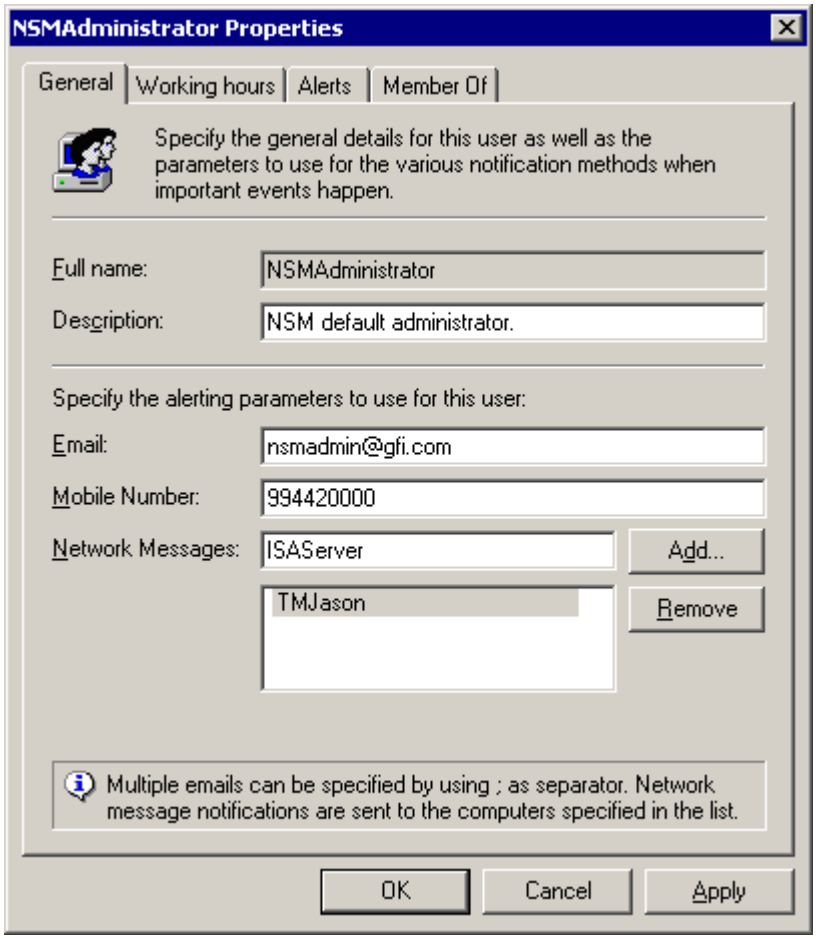
10.2.1 Add a new user

1. Right click on the Users folder under the 'Users and Groups' node and go on New > User.

2. Specify the parameters required in the user properties as described below.

Configure user properties

User parameters are defined in the user properties dialog, which opens automatically whenever a new user is being added, or can be opened when necessary by right clicking on an existing user and selecting 'Properties'.



Screenshot 134 - User Properties dialog

10.2.2 Configure user's general parameters

These parameters define the general details of the user, including the alert details (e.g. email address, SMS/Pager number, etc...), the person's working hours and the groups in which this user is a member. To configure these parameters:

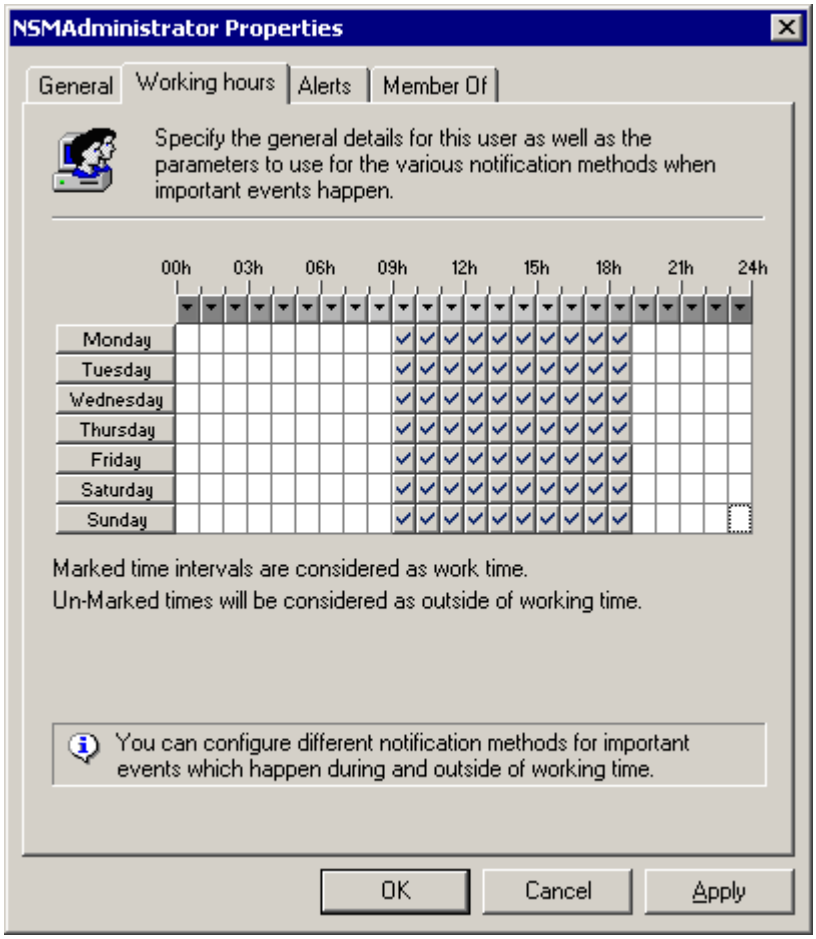
1. Click on the General tab (which is the default opening view of the user properties dialog)

2. Specify the following properties:

- *Full n*ame – Specify the full name of the user.
- Description – Specify a string which describes the user's role in the company (e.g. Mail server administrator).
- Email – Specify (if required) the address were email alerts will be sent.
- Mobile Number – Specify (if required) the mobile number were SMS alerts will be sent.
- SMS/Pager number – Specify (if required) the Pager number were SMS messages will be sent.
- Network Messages – Specify (if required) all the computers to which network messages will be sent. To add a computer to the list, type the computer name in the provided field, and then click on the 'Add' button. Repeat the same operation until all computers have been specified.

10.2.3 Define working hours

GFI Network Server Monitor, allows you to specify the working hours of a user (recipient of alerts). These parameters will be referenced by the GFI Network Server Monitor engine in order to decide what alerts (if any) need to be sent to this user, depending on the time (during or outside of working hours) that an important event occurs (e.g. a check fails).



Screenshot 135 - Working Hours Setup dialog

Marked (✓) hours indicate working time.

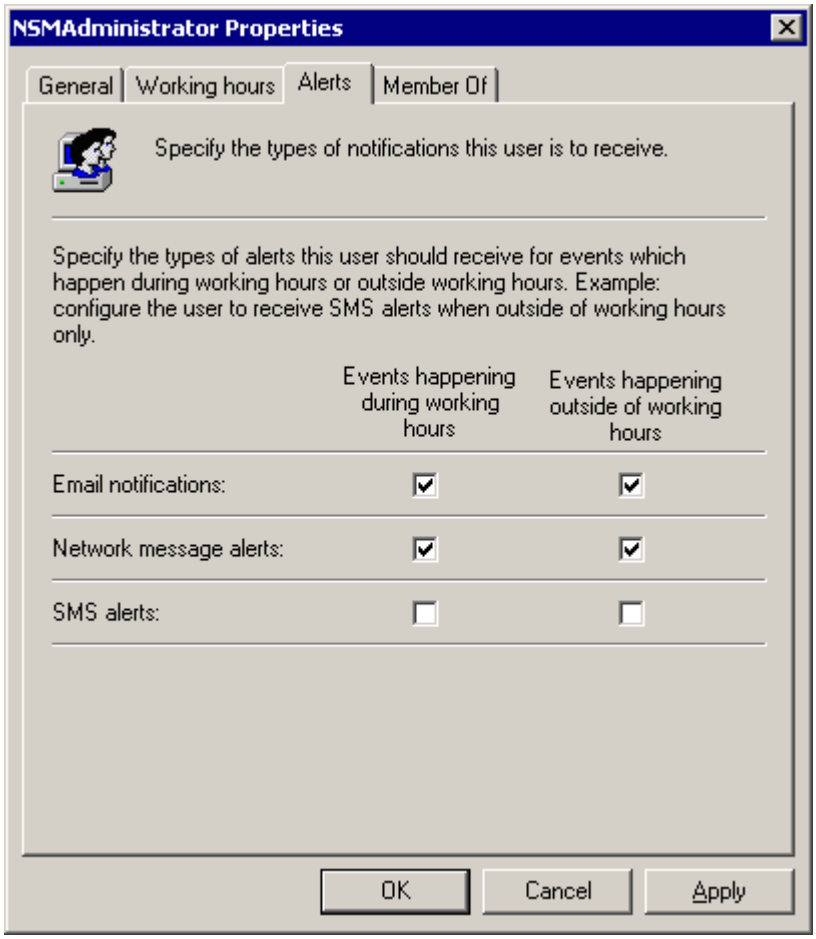
To setup working hours, click on the 'Working hours' tab and then click on the working hours that you need to mark / unmark.

TIP: To mark / unmark a whole day click on the day (e.g. MONDAY) displayed on the left of the hours setup grid.

TIP: To mark the same hour for a whole week, click on ▼ at the top of the relative hour column.

10.2.4 Define alerts to be used

You can specify what alerts (if any) are to be sent, on the occurrence of important events during and/or outside of working hours. This is based on the working hours specified for this user (e.g. you can configure GFI Network Server Monitor to send SMS/Pager alerts to this user ONLY when an event occurs outside normal working hours). For further information on how to setup the working hours for a user, please refer to the 'Working Hours' section in this chapter.


NSMAdministrator Properties
General
Working hours
Alerts
Member Of
Specify the types of notifications this user is to receive.
Specify the types of alerts this user should receive for events which happen during working hours or outside working hours. Example: configure the user to receive SMS alerts when outside of working hours only.
Events happening during working hours
Events happening outside of working hours
Email notifications:
Network message alerts:
SMS alerts:
OK
Cancel
Apply

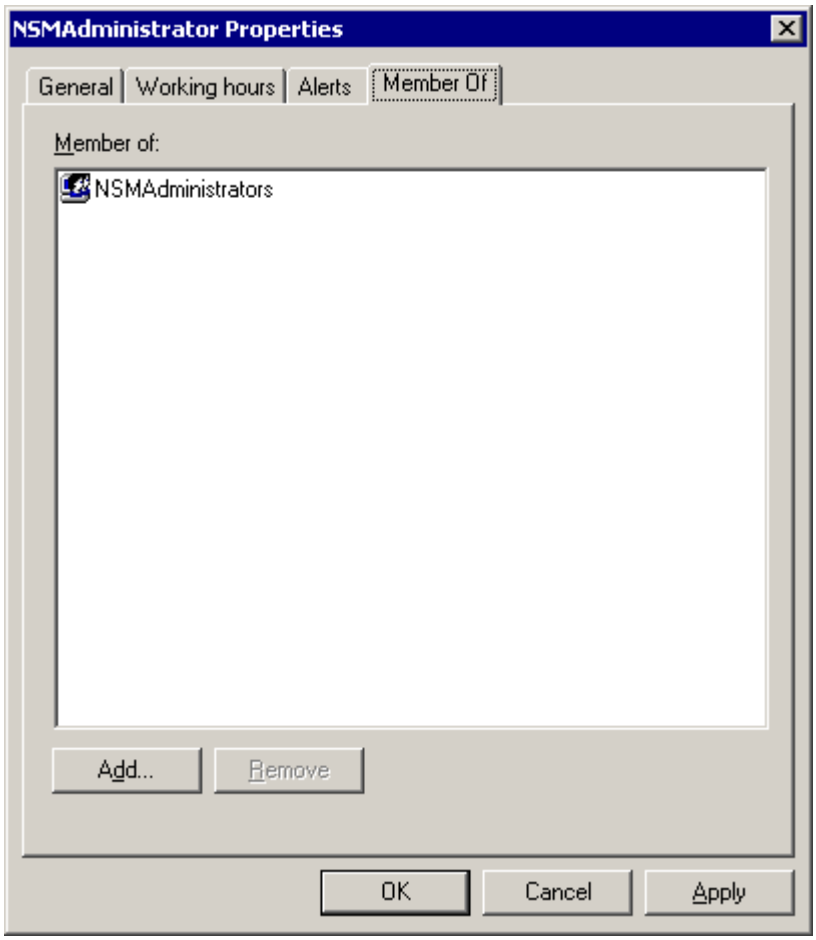
Screenshot 136- Alerts Setup Dialog

Enable the alerts that will be used when alerts occur during and/or outside of working hours (e.g. The screenshot above shows the settings for a user that will receive email alerts at any time an important event occurs as well as a Network alert if the event occurs during working hours and an SMS/Pager alert if the event occurs outside of working hours).

10.2.5 Add user to a group

A user can be added to predefined groups. You can create a group of users to notify more than 1 person and avoid having to specify multiple users for each check you create.

Users can be members of more than 1 group.



Screenshot 137- Members of tab

To specify the group(s) to which this user will be added, click on 'Add'.

TIP: You can make multiple selections of groups so as to add all required groups at one go.

10.2.6 Delete users

To delete users:

1. Click on the Users folder under the 'Users and Groups' node and select the user(s) to be deleted.

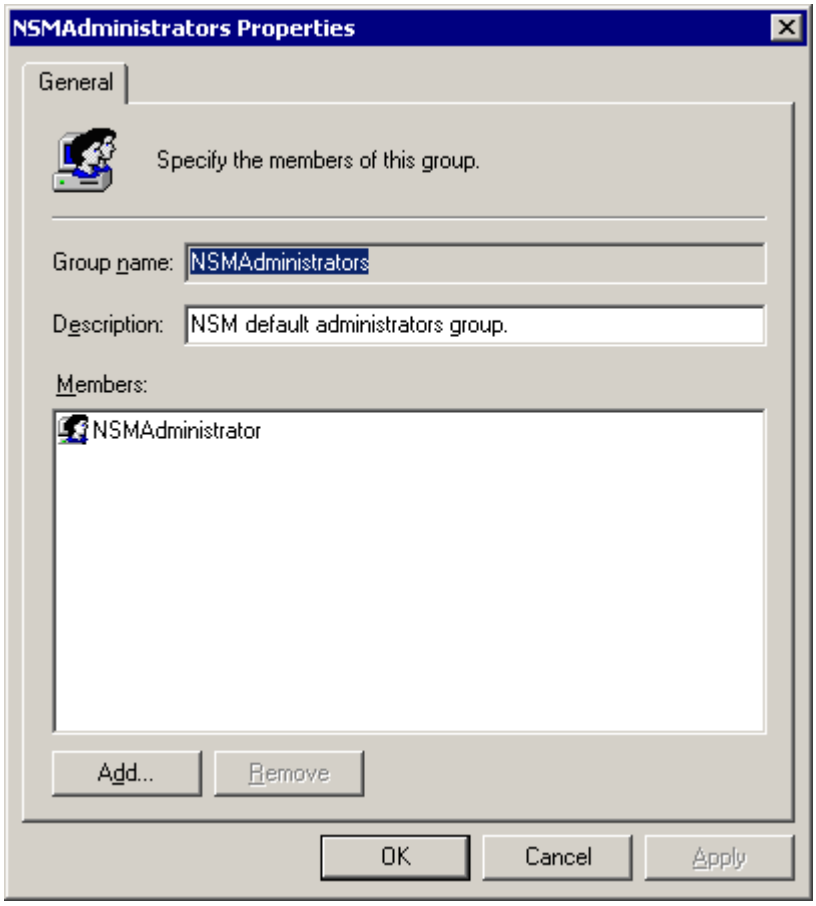
2. Right click on the selection and choose 'Delete'.

10.3 Groups

A Group contains a collection of users. You can create a group of users to notify more then 1 person and avoid having to specify multiple users for each check you create. This makes it much easier to add new alert recipients to that particular check since you just need to associate the new users to the recipients group.

10.3.1 Add a new group

1. Click on the Group folder under the 'Users and Groups' node and go on NEW > GROUP.



Screenshot 138 - Group Properties dialog

2. Specify the group name (e.g. NetworkAdministrators) and the string which describes the group/groups members (e.g. File Server Administrator).

3. To specify the members for this group, click on ‘Add’, select the users and click on ‘OK’ to accept the selection.

10.3.2 Add members to an existing group

To add users to an existing group:

1. Double click on the Group folder under the ‘Users and Groups’ node, right click on the group were the new member will be added and select ‘Properties’.

2. Click on the ‘Add’ button, select the new members and click on ‘OK’ to accept the selection.

10.3.3 Remove members from a group

1. Double click on the Group folder under the ‘Users and Groups’ node, right click on the group were the new member will be added and select ‘Properties’.

2. Select members to be deleted from displayed list and click on ‘Remove’.

10.3.4 Delete a group

Double click on the Group folder under the ‘Users and Groups’ node, right click on the group to be deleted and select ‘Delete’.

11 Reporting

11.1 Introduction

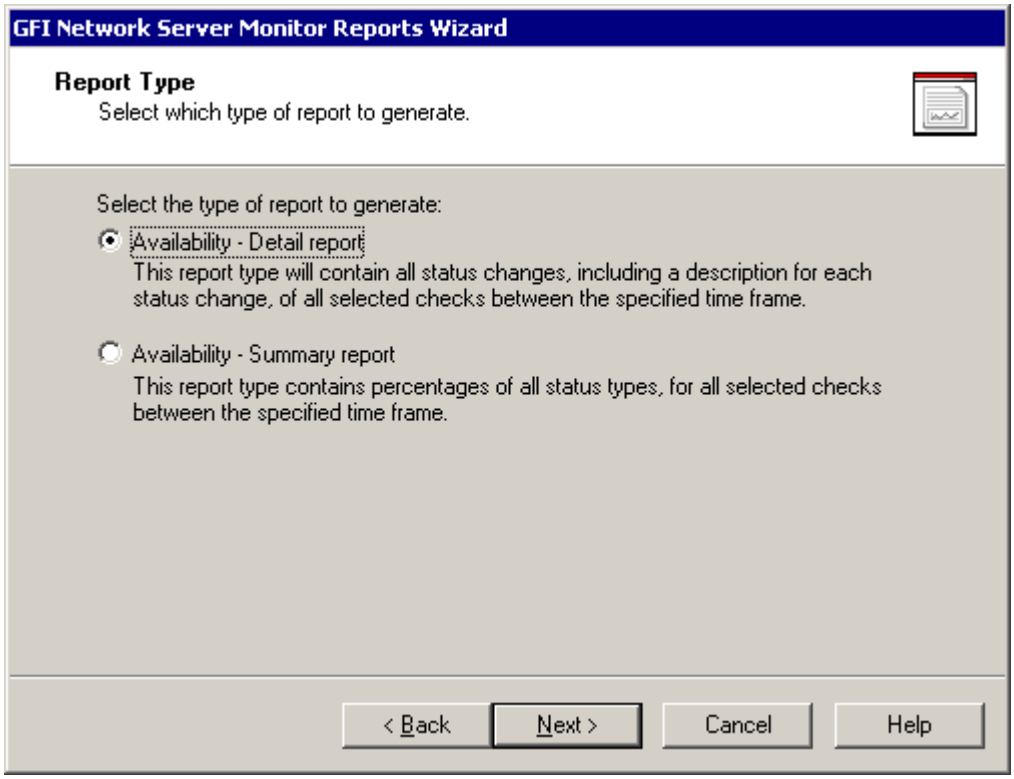
Out of the box, GFI Network Server Monitor includes a dedicated reporting tool. This tool allows you to create reports that detail the availability of your network resources. You can create reports directly in HTML, or generate XML/CSV reports that you can export to your favorite application. You can use the report templates included in GFI Network Server Monitor to extract monitor data from the database backend and generate detailed or summary reports based on a particular period of time.

11.2 Availability - Detail Report

The Availability-Detail Report includes an overview of all changes in check state that occurred across a specified period of time. Other details included in this report specify the length of time a server or service was in a particular state, making it easy to define the relative up/down time.

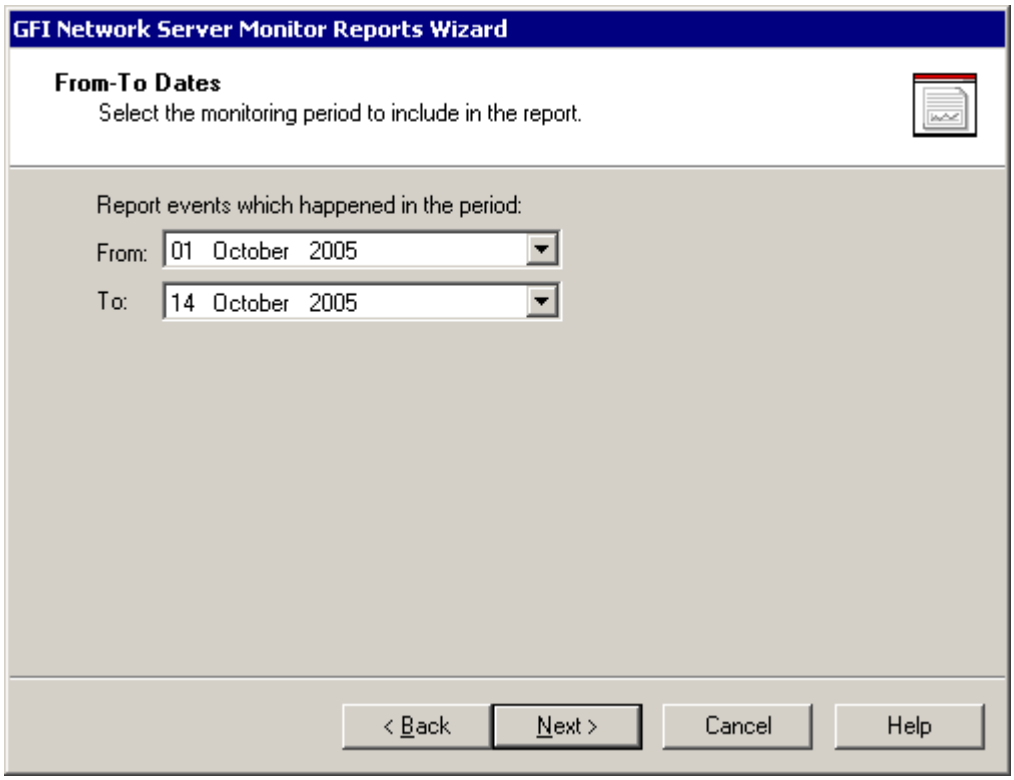
To generate an Availability-Detail Report:

1. Go on Start > GFI Network Server Monitor 7 program group > GFI N.S.M. 7 Reporter. This launches the Reports Wizard. Click on 'Next' to start creating the report.


GFI Network Server Monitor Reports Wizard
Report Type
Select which type of report to generate.
Select the type of report to generate:
Availability - Detail report
This report type will contain all status changes, including a description for each status change, of all selected checks between the specified time frame.
Availability - Summary report
This report type contains percentages of all status types, for all selected checks between the specified time frame.
< Back
Next >
Cancel
Help

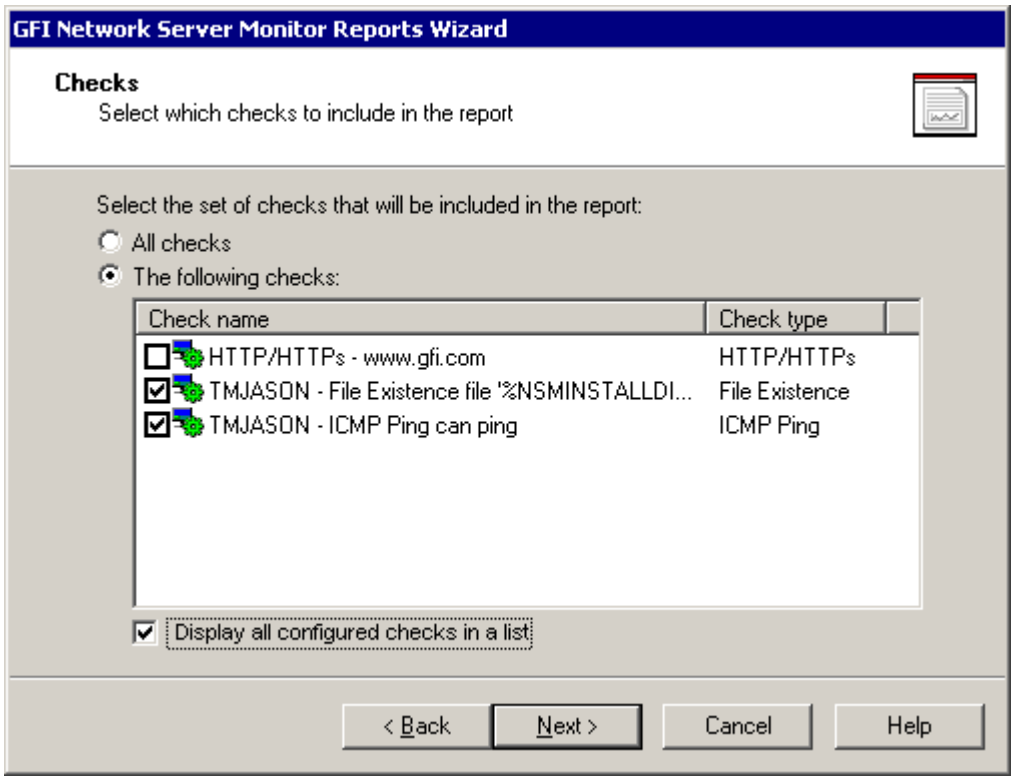
Screenshot 139 - Specify report interval

2. Select the 'Availability-*Detail Report*' option and click on 'Next' to continue.


GFI Network Server Monitor Reports Wizard
From-To Dates
Select the monitoring period to include in the report.
Report events which happened in the period:
From: 01 October 2005
To: 14 October 2005
< Back
Next >
Cancel
Help

Screenshot 140 - Select the period to be covered by report

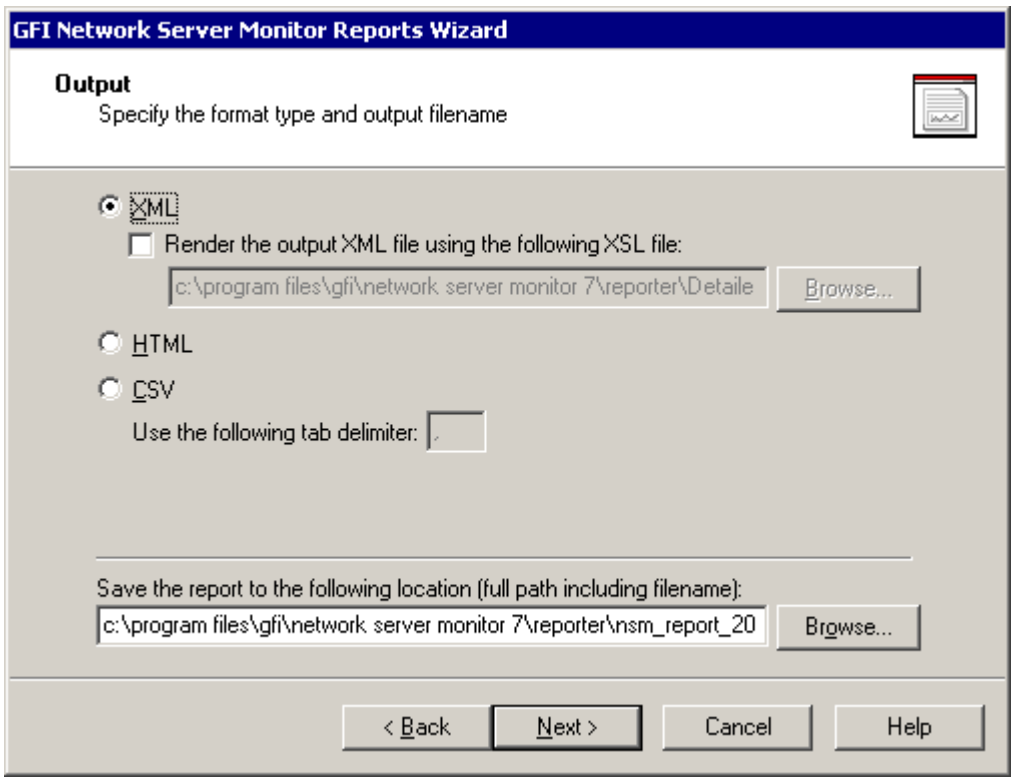
3. Specify the monitoring period ('From:' and 'To:' date) to be covered by the report.



Screenshot 141 - Specify which checks to include in the report

4. Specify the checks that you wish to include in your report. Select the *'All Checks'* option to include the data of all existing checks. Alternatively you can select *'The following checks:'* option and choose the checks which you wish to include in the report. When ready, click on 'Next' to continue.

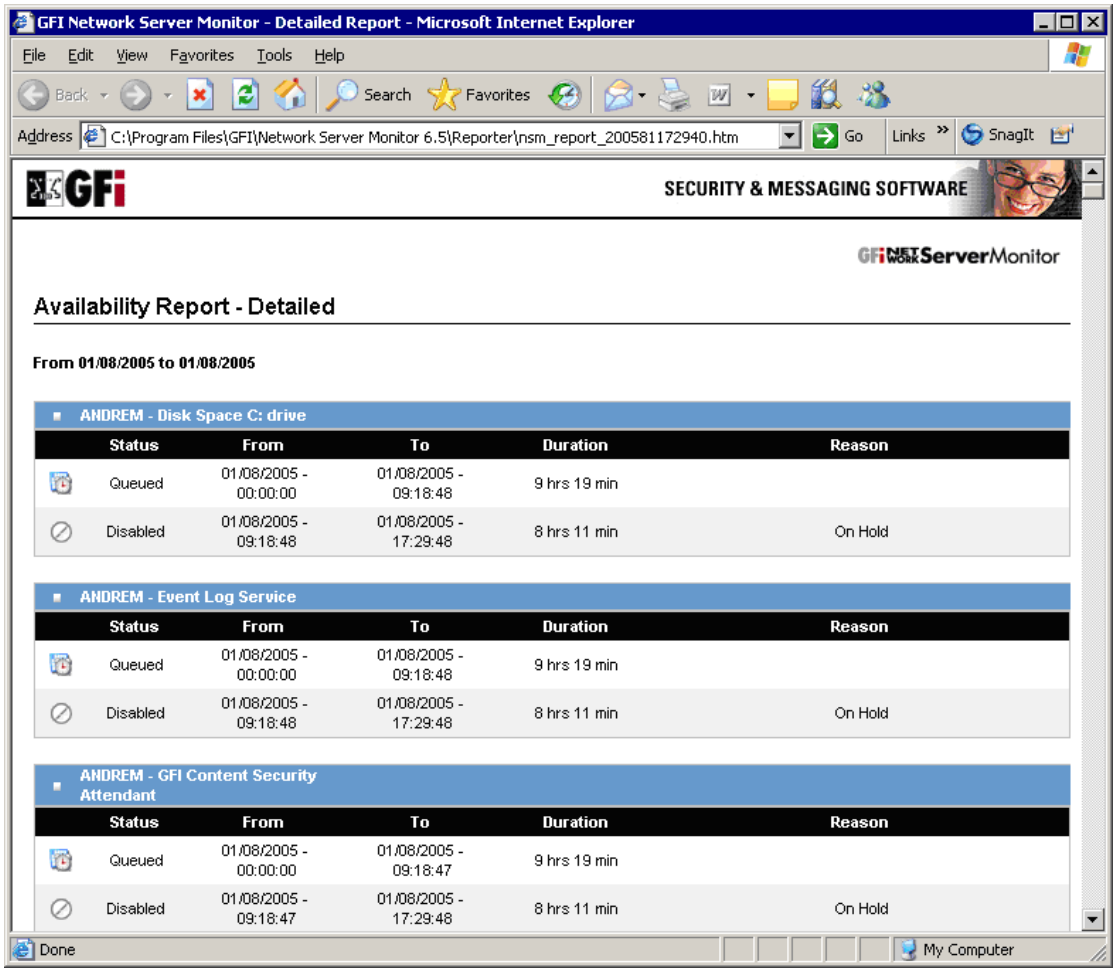
By default checks are listed in their respective folders. To display only the list of currently configured checks (i.e. without folders), select the *'Display all configured checks in a list'* option.



Screenshot 142 - Choose the report format required

5. Specify the format type and output file name of the report. Select *'CSV'* or *'XML'* formats if you want to further process the report and perform more advanced calculations using another (external) program such as Microsoft Excel. Click on 'Next' to continue.

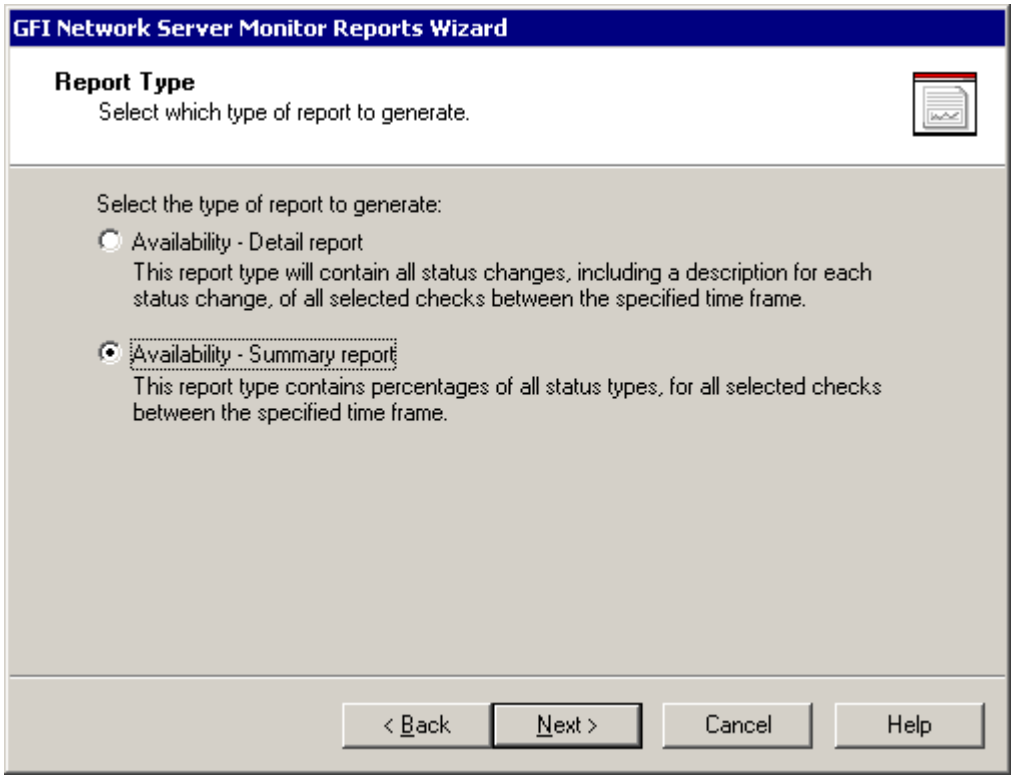
6. At the final stage, a dialog will inform you that the report wizard is ready to start generating the report. If you want to modify any of the previously configured settings, click on 'Back'. Otherwise, click on 'Next' to finalize the report.


GFI Network Server Monitor - Detailed Report - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address C:\Program Files\GFI\Network Server Monitor 6.5\Reporter\nsm_report_200581172940.htm
Go Links SnagIt
GFI
SECURITY & MESSAGING SOFTWARE
GFI NETWORK ServerMonitor
Availability Report - Detailed
From 01/08/2005 to 01/08/2005
ANDREM - Disk Space C: drive
Status From To Duration Reason
Queued 01/08/2005 - 00:00:00 01/08/2005 - 09:18:48 9 hrs 19 min
Disabled 01/08/2005 - 09:18:48 01/08/2005 - 17:29:48 8 hrs 11 min On Hold
ANDREM - Event Log Service
Status From To Duration Reason
Queued 01/08/2005 - 00:00:00 01/08/2005 - 09:18:48 9 hrs 19 min
Disabled 01/08/2005 - 09:18:48 01/08/2005 - 17:29:48 8 hrs 11 min On Hold
ANDREM - GFI Content Security Attendant
Status From To Duration Reason
Queued 01/08/2005 - 00:00:00 01/08/2005 - 09:18:47 9 hrs 19 min
Disabled 01/08/2005 - 09:18:47 01/08/2005 - 17:29:48 8 hrs 11 min On Hold
Done
My Computer

Screenshot 143 - The availability detailed report

11.3 Availability-Summary Report

The Availability-Summary Report contains information showing the state of target computers over a specified period of time.

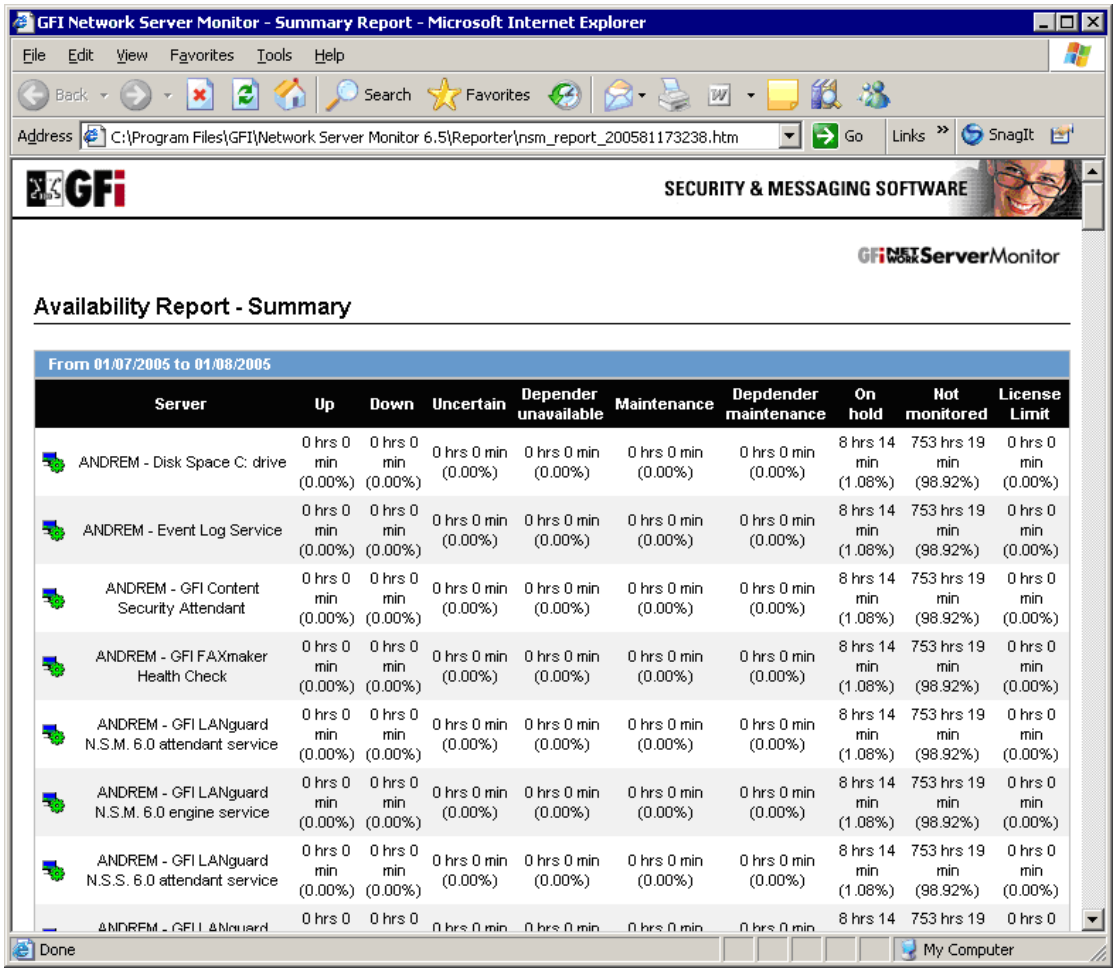

GFI Network Server Monitor Reports Wizard
Report Type
Select which type of report to generate.
Select the type of report to generate:
Availability - Detail report
This report type will contain all status changes, including a description for each status change, of all selected checks between the specified time frame.
Availability - Summary report
This report type contains percentages of all status types, for all selected checks between the specified time frame.
< Back
Next >
Cancel
Help

Screenshot 144 - First Stage of the report wizard: Report Type dialog

To generate an Availability-Summary Report:

1. Launch the report wizard and select the 'Availability–Summary Report' option.

2. Specify the rest of the required settings in the same way as described for the creation of an Availability-Detail Report. For more information, refer to the Availability-Detail Report section in this chapter.


GFI Network Server Monitor - Summary Report - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address C:\Program Files\GFI\Network Server Monitor 6.5\Reporter\nsm_report_200581173238.htm
Go Links SnagIt
GFI
SECURITY & MESSAGING SOFTWARE
GFI NETWORK ServerMonitor
Availability Report - Summary
From 01/07/2005 to 01/08/2005
Server | Up | Down | Uncertain | Depender unavailable | Maintenance | Depdender maintenance | On hold | Not monitored | License Limit
ANDREM - Disk Space C: drive | 0 hrs 0 min (0.00%) | 0 hrs 0 min (0.00%) | 0 hrs 0 min (0.00%) | 0 hrs 0 min (0.00%) | 0 hrs 0 min (0.00%) | 0 hrs 0 min (0.00%) | 8 hrs 14 min (1.08%) | 753 hrs 19 min (98.92%) | 0 hrs 0 min (0.00%)
ANDREM - Event Log Service | 0 hrs 0 min (0.00%) | 0 hrs 0 min (0.00%) | 0 hrs 0 min (0.00%) | 0 hrs 0 min (0.00%) | 0 hrs 0 min (0.00%) | 0 hrs 0 min (0.00%) | 8 hrs 14 min (1.08%) | 753 hrs 19 min (98.92%) | 0 hrs 0 min (0.00%)
ANDREM - GFI Content Security Attendant | 0 hrs 0 min (0.00%) | 0 hrs 0 min (0.00%) | 0 hrs 0 min (0.00%) | 0 hrs 0 min (0.00%) | 0 hrs 0 min (0.00%) | 0 hrs 0 min (0.00%) | 8 hrs 14 min (1.08%) | 753 hrs 19 min (98.92%) | 0 hrs 0 min (0.00%)
ANDREM - GFI FAXmaker Health Check | 0 hrs 0 min (0.00%) | 0 hrs 0 min (0.00%) | 0 hrs 0 min (0.00%) | 0 hrs 0 min (0.00%) | 0 hrs 0 min (0.00%) | 0 hrs 0 min (0.00%) | 8 hrs 14 min (1.08%) | 753 hrs 19 min (98.92%) | 0 hrs 0 min (0.00%)
ANDREM - GFI LANguard N.S.M. 6.0 attendant service | 0 hrs 0 min (0.00%) | 0 hrs 0 min (0.00%) | 0 hrs 0 min (0.00%) | 0 hrs 0 min (0.00%) | 0 hrs 0 min (0.00%) | 0 hrs 0 min (0.00%) | 8 hrs 14 min (1.08%) | 753 hrs 19 min (98.92%) | 0 hrs 0 min (0.00%)
ANDREM - GFI LANguard N.S.M. 6.0 engine service | 0 hrs 0 min (0.00%) | 0 hrs 0 min (0.00%) | 0 hrs 0 min (0.00%) | 0 hrs 0 min (0.00%) | 0 hrs 0 min (0.00%) | 0 hrs 0 min (0.00%) | 8 hrs 14 min (1.08%) | 753 hrs 19 min (98.92%) | 0 hrs 0 min (0.00%)
ANDREM - GFI LANguard N.S.S. 6.0 attendant service | 0 hrs 0 min (0.00%) | 0 hrs 0 min (0.00%) | 0 hrs 0 min (0.00%) | 0 hrs 0 min (0.00%) | 0 hrs 0 min (0.00%) | 0 hrs 0 min (0.00%) | 8 hrs 14 min (1.08%) | 753 hrs 19 min (98.92%) | 0 hrs 0 min (0.00%)
Done
My Computer

Screenshot 145 - The availability summary report

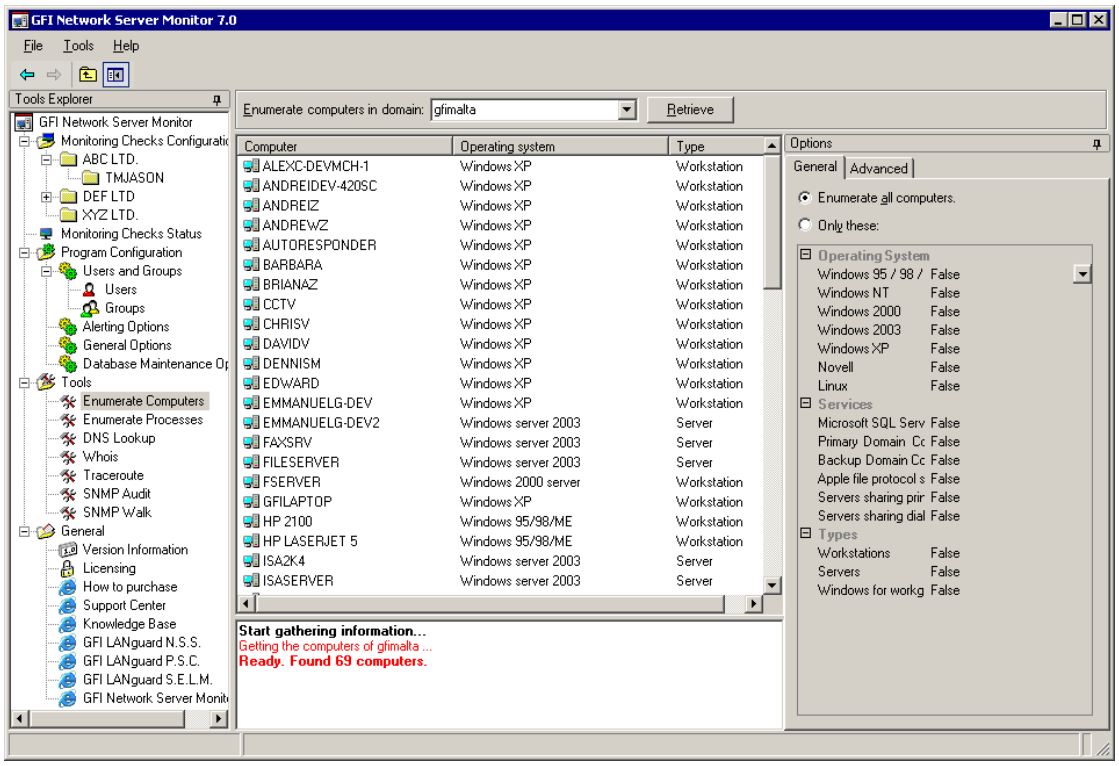
12 Network tools

12.1 Enumerate computers

This tool searches for domains and/or workgroups on your network. Once the domains are defined, you can scan their contents to catalog the constituent computers and their relative details (e.g., OS, other information from NETBIOS). Computers can be enumerated from:

- The Active Directory – Fast method which will also enumerate computers that are currently switched off.
- The Windows Explorer interface – This method is slower and will not enumerate computers that are switched off.

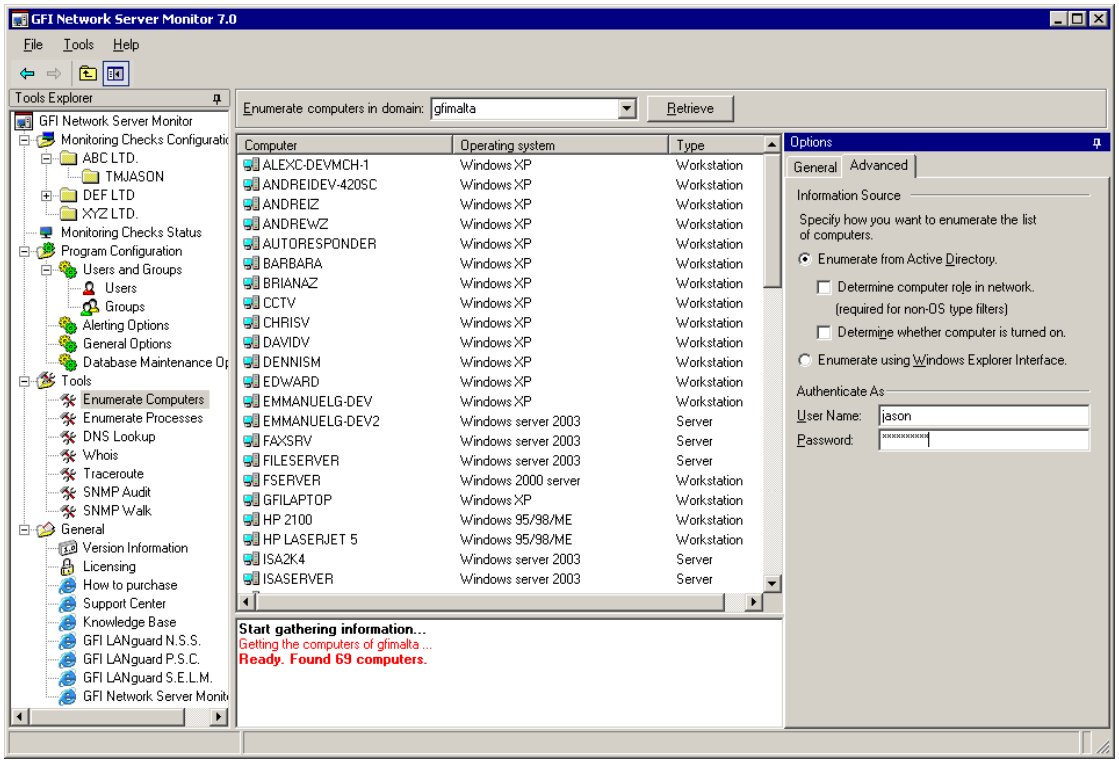
When performing scans, you must use access accounts that have rights over the Active Directory.



Screenshot 146 - Enumerate computers - General Tab options

To setup the required parameters:

1. Click on the general tab.
2. Specify the domain where a search is to be made (e.g. GFIMALTA).
3. Specify the computers which need to be listed:
   - Select 'Enumerate All computers' to display all computers in the domain.
   - Select 'Only these' to specify which computers to look for. Define selection criteria parameters to be used from the Operating System, Computer services and Computer type options available.
4. Click on the 'Advanced Tab' and choose the search method by marking '*Enumerate from Active directory' or 'Enumerate using Windows Explore Interface'*



Screenshot 147 - Enumerate Computers - Advanced tab options

5. Define additional information to be displayed by marking 'Determine Computer role on the network' and/or 'Determine whether computer is turned on'.

Should it be required, enter authentication details in the fields located at the bottom.

The list of constituent computers in the specified domain will be displayed. Status details of the operation carried out is displayed in the bottom window

E.g. To look for ALL computers which run on Windows 2003 OS in a domain called JASONTEST:

(a) Select / enter domain name.

(b) Click on the 'General' tab, enable 'Only these' option.

(c) Set to 'True' the value near Windows 2003 in the Operating System selection area.

(d) Click on the 'Advanced' Tab

(e) Enable 'Enumerate from Active Directory' as well as 'Determine computer role in network' and 'Determine *whether computer is on*'.

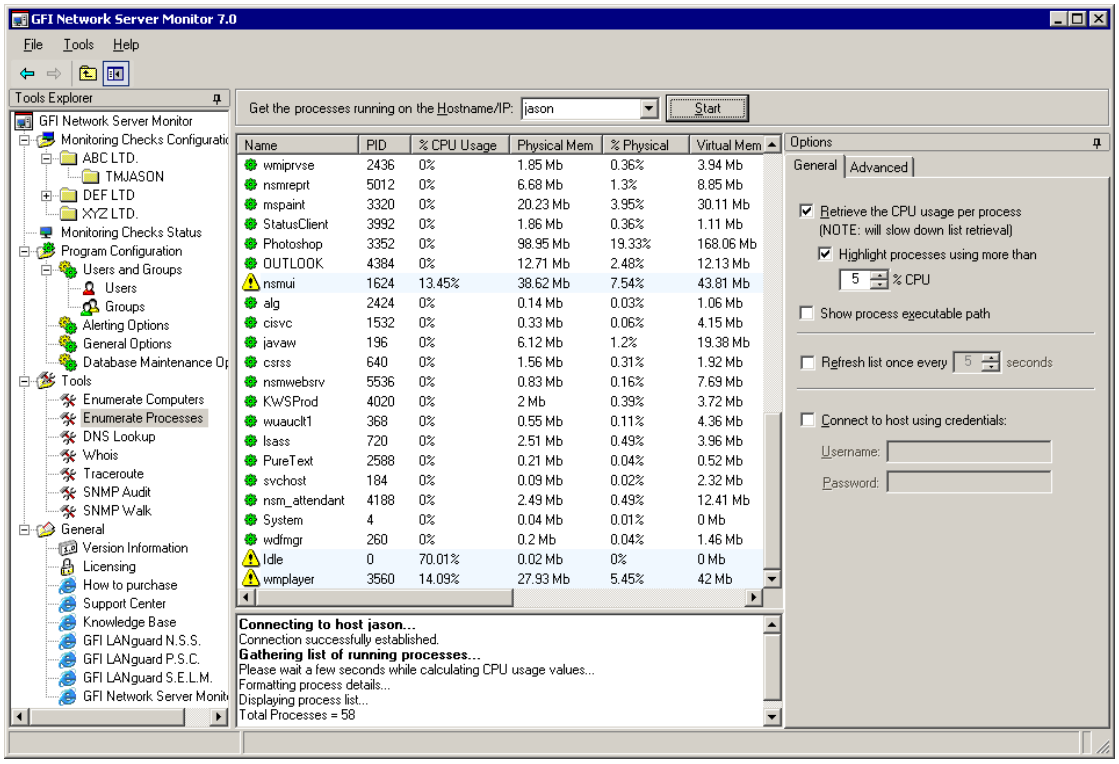
6. Click on 'Retrieve' to start enumerating computers.

12.2 Enumerate processes

This tool is used to catalog processes running on a remote computer. Amongst other tasks, this tool searches and displays information on the CPU and Memory resources consumed by each process found running on the specified target computer. You can also highlight / a particular process or indicate processes which are consuming more than a defined percentage (%) of CPU usage. The set up window layout is similar to the enumerate computer's tool, were the resulting list of processes is displayed in the top-middle window, whilst the status/details of the operation carried out are displayed in the bottom-middle window. Icons on the left of each process indicate the state of the process in relation to the specified CPU usage value.

Indicates that the process is using more than the specified CPU usage limit.

Indicates that the process is using less CPU resources than the specified limit.


GFI Network Server Monitor 7.0
File Tools Help
Tools Explorer
GFI Network Server Monitor
Monitoring Checks Configurati
ABC LTD.
TMJASON
DEF LTD
XYZ LTD.
Monitoring Checks Status
Program Configuration
Users and Groups
Users
Groups
Alerting Options
General Options
Database Maintenance Op
Tools
Enumerate Computers
Enumerate Processes
DNS Lookup
Whois
Traceroute
SNMP Audit
SNMP Walk
General
Version Information
Licensing
How to purchase
Support Center
Knowledge Base
GFI LANguard N.S.S.
GFI LANguard P.S.C.
GFI LANguard S.E.L.M.
GFI Network Server Monit
Get the processes running on the Hostname/IP: jason
Start
Name PID % CPU Usage Physical Mem % Physical Virtual Mem
wmiprvse 2436 0% 1.85 Mb 0.36% 3.94 Mb
nsmreprt 5012 0% 6.68 Mb 1.3% 8.85 Mb
mspaint 3320 0% 20.23 Mb 3.95% 30.11 Mb
StatusClient 3992 0% 1.86 Mb 0.36% 1.11 Mb
Photoshop 3352 0% 98.95 Mb 19.33% 168.06 Mb
OUTLOOK 4384 0% 12.71 Mb 2.48% 12.13 Mb
nsmui 1624 13.45% 38.62 Mb 7.54% 43.81 Mb
alg 2424 0% 0.14 Mb 0.03% 1.06 Mb
cisvc 1532 0% 0.33 Mb 0.06% 4.15 Mb
javaw 196 0% 6.12 Mb 1.2% 19.38 Mb
csrss 640 0% 1.56 Mb 0.31% 1.92 Mb
nsmwebsrv 5536 0% 0.83 Mb 0.16% 7.69 Mb
KWSProd 4020 0% 2 Mb 0.39% 3.72 Mb
wuauclt1 368 0% 0.55 Mb 0.11% 4.36 Mb
lsass 720 0% 2.51 Mb 0.49% 3.96 Mb
PureText 2588 0% 0.21 Mb 0.04% 0.52 Mb
svchost 184 0% 0.09 Mb 0.02% 2.32 Mb
nsm_attendant 4188 0% 2.49 Mb 0.49% 12.41 Mb
System 4 0% 0.04 Mb 0.01% 0 Mb
wdfmgr 260 0% 0.2 Mb 0.04% 1.46 Mb
Idle 0 70.01% 0.02 Mb 0% 0 Mb
wmplayer 3560 14.09% 27.93 Mb 5.45% 42 Mb
Connecting to host jason...
Connection successfully established.
Gathering list of running processes...
Please wait a few seconds while calculating CPU usage values...
Formatting process details...
Displaying process list...
Total Processes = 58
Options
General Advanced
Retrieve the CPU usage per process
(NOTE: will slow down list retrieval)
Highlight processes using more than
5 % CPU
Show process executable path
Refresh list once every 5 seconds
Connect to host using credentials:
Username:
Password:

Screenshot 148 - Enumerate Processes setup window - General Tab

This tool requires the following parameters in the 'General' tab view:

- Hostname/IP – The name of the remote computer whose processes will be enumerated.
- Retrieve CPU usage per process – Indicate that the process list should include the percentage (%) CPU usage value.
- CPU % usage – Specify the maximum percentage (%) CPU usage allowed. This option will then highlight processes using more than the specified limit.
- Refresh list frequency – Specify the time interval in seconds, at which the list of processes will be refreshed.
- Logon Credentials – Specify logon credentials (if any), required to connect to host computers.

The following parameters are required in the 'Advanced' tab view:

- Highlight processes – Specify the list of processes which you need to highlight in the derived list of processes. This is convenient to find any known unwanted process, such as viruses, which are running on a remote computer, or vice versa to confirm if a particular process, such as a virus, shield is running.
- Hide Processes – Specify the list of processes that you do not want to display in the derived list of processes.

To retrieve the list of running processes:

1. Specify the name/IP of the computer from where to retrieve the processes.

2. Specify if you want to display the percentage (%) CPU usage and indicate if processes using more than a specified CPU usage value are to be highlighted. Specify the percentage (%) CPU usage value to be used as reference.

3. Set the refresh rate at which the list will be updated.

4. Specify logon authentication details (if any).

5. To highlight particular processes, click on the 'Advanced' tab and specify the process names, one for each line. The specified processes will be highlighted in yellow and displayed in the list.

6. To hide any known processes from being displayed click on the 'Advanced' tab and specify the process names in the 'Hide processes 'list, one process per line.

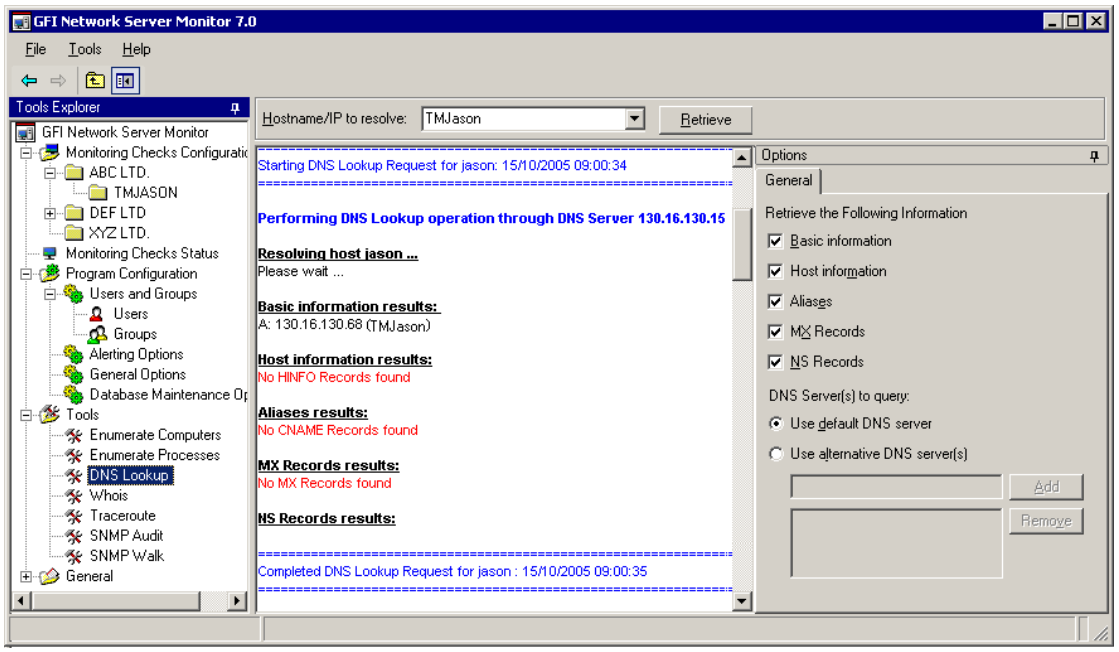
7. Click on ‘Start’ to start enumerating processes.

Name	PID	% CPU Usage	Physical Mem	% Physical	Virtual Mem
wmiprvse	2436	0%	1.85 Mb	0.36%	3.94 Mb
nsmreprt	5012	0%	6.68 Mb	1.3%	8.85 Mb
mspaint	3320	0%	20.23 Mb	3.95%	30.11 Mb
StatusClient	3992	0%	1.86 Mb	0.36%	1.11 Mb
Photoshop	3352	0%	98.95 Mb	19.33%	168.06 Mb
OUTLOOK	4384	0%	12.71 Mb	2.48%	12.13 Mb
nsmui	1624	13.45%	38.62 Mb	7.54%	43.81 Mb
alg	2424	0%	0.14 Mb	0.03%	1.06 Mb
cisvc	1532	0%	0.33 Mb	0.06%	4.15 Mb
javaw	196	0%	6.12 Mb	1.2%	19.38 Mb
csrss	640	0%	1.56 Mb	0.31%	1.92 Mb
nsmwebsrv	5536	0%	0.83 Mb	0.16%	7.69 Mb
KWSProd	4020	0%	2 Mb	0.39%	3.72 Mb
wuauclt1	368	0%	0.55 Mb	0.11%	4.36 Mb
lsass	720	0%	2.51 Mb	0.49%	3.96 Mb
PureText	2588	0%	0.21 Mb	0.04%	0.52 Mb
svchost	184	0%	0.09 Mb	0.02%	2.32 Mb
nsm_attendant	4188	0%	2.49 Mb	0.49%	12.41 Mb
System	4	0%	0.04 Mb	0.01%	0 Mb
wdfmgr	260	0%	0.2 Mb	0.04%	1.46 Mb
Idle	0	70.01%	0.02 Mb	0%	0 Mb
wmplayer	3560	14.09%	27.93 Mb	5.45%	42 Mb

Screenshot 149 - List of Highlighted Processes

12.3 DNS lookup

This tool helps resolving domain names to their corresponding IP address. During the DNS lookup process, this tool also enumerates additional information such as Aliases, MX and NS Records.



Screenshot 150- DNS Lookup - setup Window

To obtain information about a domain name:

1. Go to the Tools > ‘DNS lookup’ node.
2. Specify the hostname to resolve.

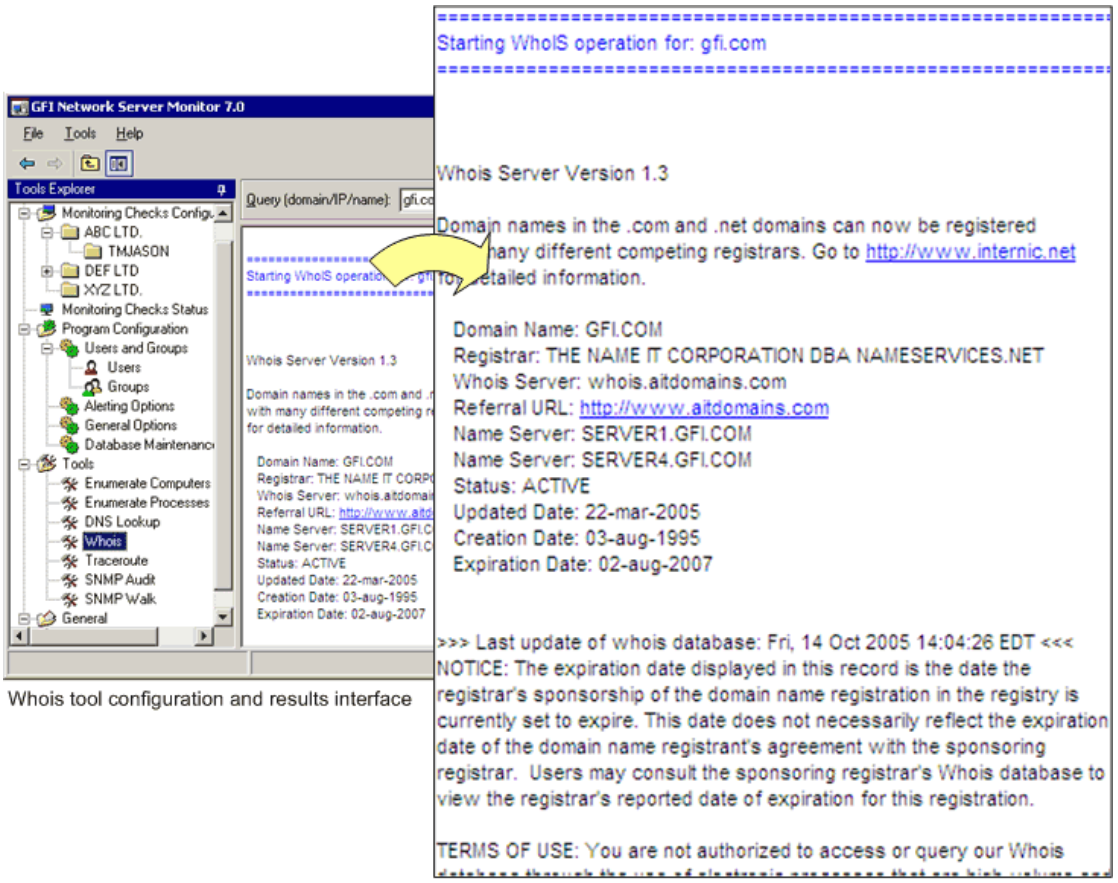
3. Specify the information to be retrieved.

- Basic Information – i.e. host name and what IP this resolves.
- Host Information - known technically as the HINFO, usually includes information such as hardware and what OS runs on the specified domain (most DNS entries do not contain this information for security reasons).
- Aliases - return information on any A Records the Domain might have.
- MX Records - known also as Mail exchangers records, show which mail server(s) in order, are responsible for this domain.
- NS Records - indicate which name servers are responsible for this domain.

In addition it is possible to specify alternative DNS servers.

12.4 Whois

This tool looks up information on a domain or IP address. You can select a specific Whois Server from the options area, or you can use the 'Default' option which will select a server for you.


GFI Network Server Monitor 7.0
File Tools Help
Tools Explorer
Monitoring Checks Config.
ABC LTD.
TMJASON
DEF LTD
XYZ LTD.
Monitoring Checks Status
Program Configuration
Users and Groups
Users
Groups
Alerting Options
General Options
Database Maintenanc
Tools
Enumerate Computers
Enumerate Processes
DNS Lookup
Whois
Traceroute
SNMP Audit
SNMP Walk
General
Query (domain/IP/name):
Starting WhoIS operation for: gfi.com
Whois Server Version 1.3
Domain Name: GFI.COM
Registrar: THE NAME IT CORPORATION DBA NAMESERVICES.NET
Whois Server: whois.aitdomains.com
Referral URL: http://www.aitdomains.com
Name Server: SERVER1.GFI.COM
Name Server: SERVER4.GFI.COM
Status: ACTIVE
Updated Date: 22-mar-2005
Creation Date: 03-aug-1995
Expiration Date: 02-aug-2007
>>> Last update of whois database: Fri, 14 Oct 2005 14:04:26 EDT <<<
NOTICE: The expiration date displayed in this record is the date the registrar's sponsorship of the domain name registration in the registry is currently set to expire. This date does not necessarily reflect the expiration date of the domain name registrant's agreement with the sponsoring registrar. Users may consult the sponsoring registrar's Whois database to view the registrar's reported date of expiration for this registration.
TERMS OF USE: You are not authorized to access or query our Whois

Whois tool configuration and results interface

Whois query results

Screenshot 151 - Whois tool results

1. Specify the parameters required for this tool:

- *Domain* Name/IP Address – The hostname/IP to resolve and retrieve details for.
- Whois Server – The server which will process the query and supply the information related to the defined host.

2. Click on 'Retrieve' to start the search.

12.5 Traceroute

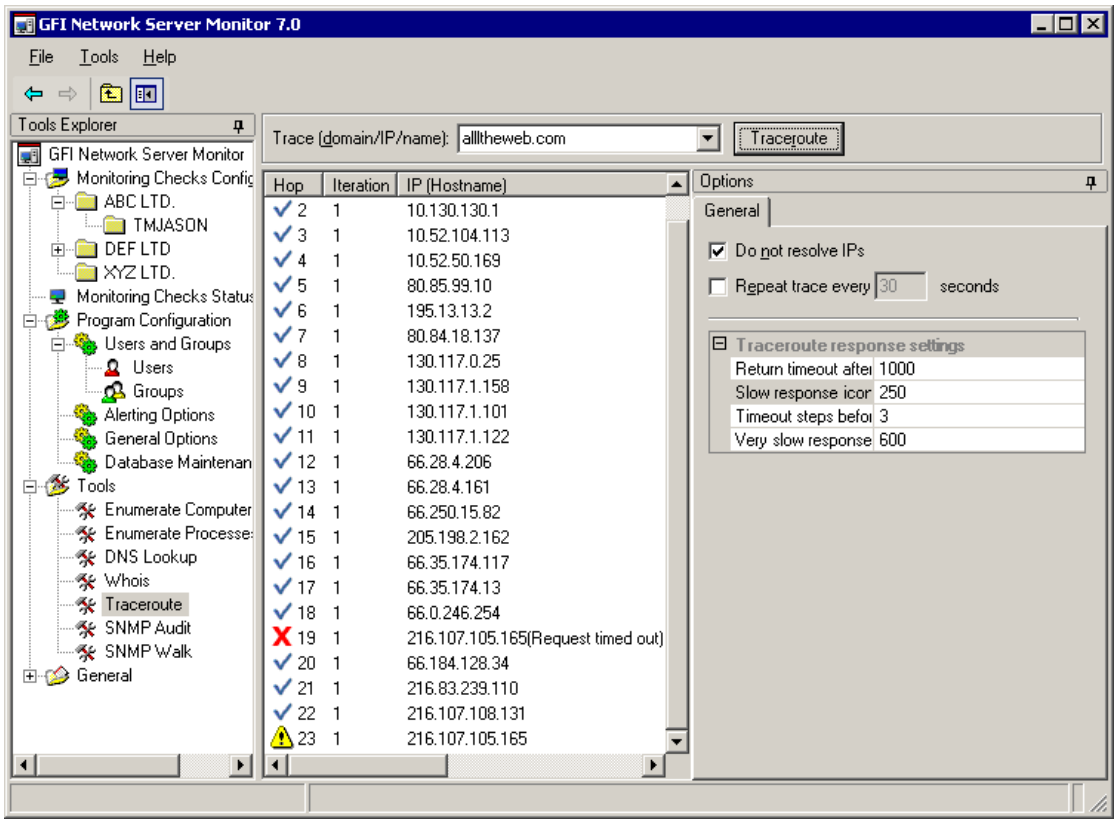
This tool shows the network path that GFI Network Server Monitor followed to reach the target computer. When you perform a trace route, each hop has an icon next to it which indicates:

A successful hop taken within normal parameters.

A successful hop, but time required was quite long.

A successful hop, but the time required was too long.

The hop failed / timed out. (i.e. it took longer then 1000ms).



Screenshot 152 - Traceroute Setup window

1. Specify the following parameters:

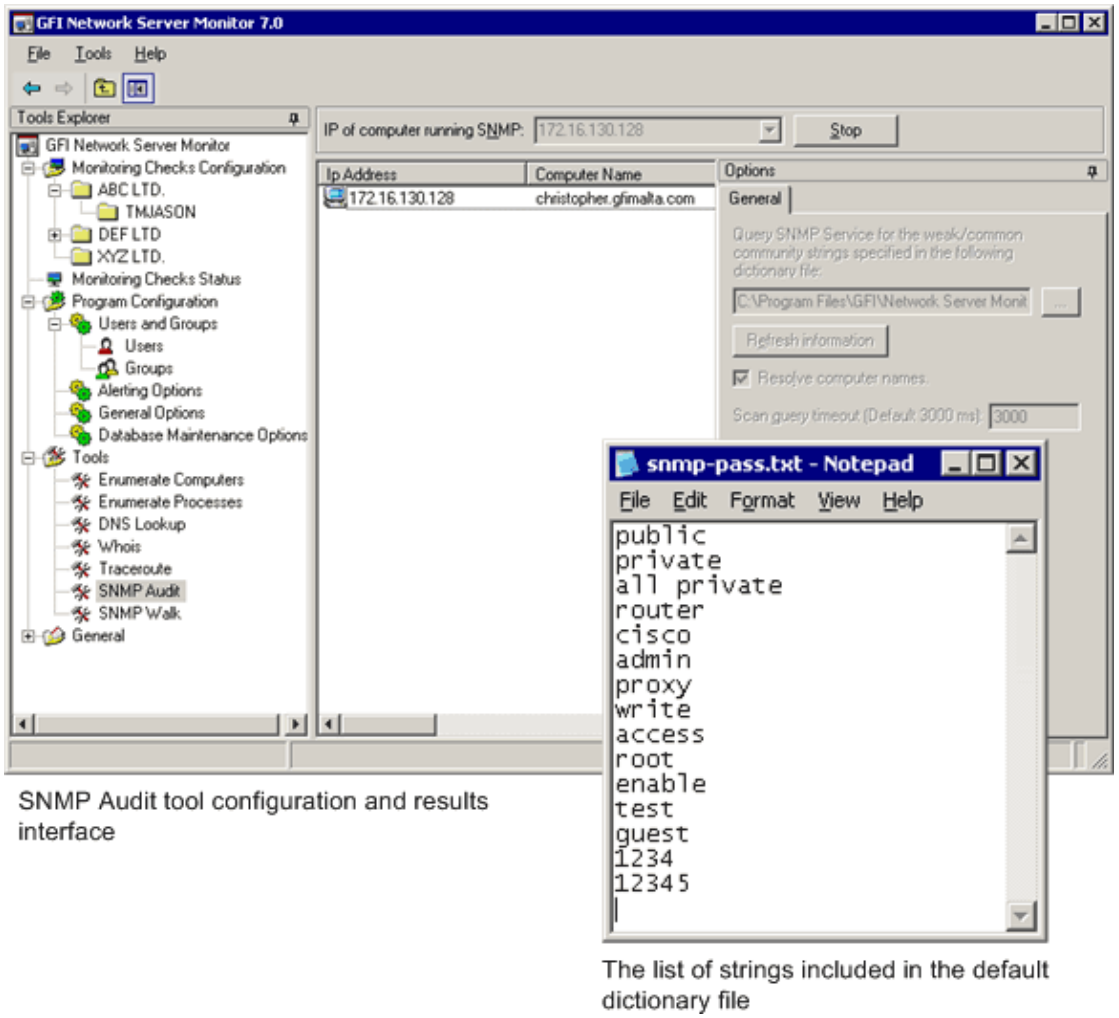
   - Domain/IP/Name – Specify the targeted destination.
   - Do Not resolve IPs – Enable this flag to indicate that only the IP Address is required to be displayed.
   - Repetition Frequency - Define if the function is to be run more than once and specify the interval between each run.

2. Click on 'Traceroute' to start the trace.

12.6 SNMP audit

The SNMP audit tool, allows you to perform an SNMP audit on a device and audit for weak community strings.

Some network devices will have alternative or non-default community strings. The dictionary file contains a list of popular community strings to check for. The default file it uses for the dictionary attack is called snmp-pass.txt. You can either add new community names to this file, or direct the SNMP audit to use another file altogether.



SNMP Audit tool configuration and results interface

The list of strings included in the default dictionary file

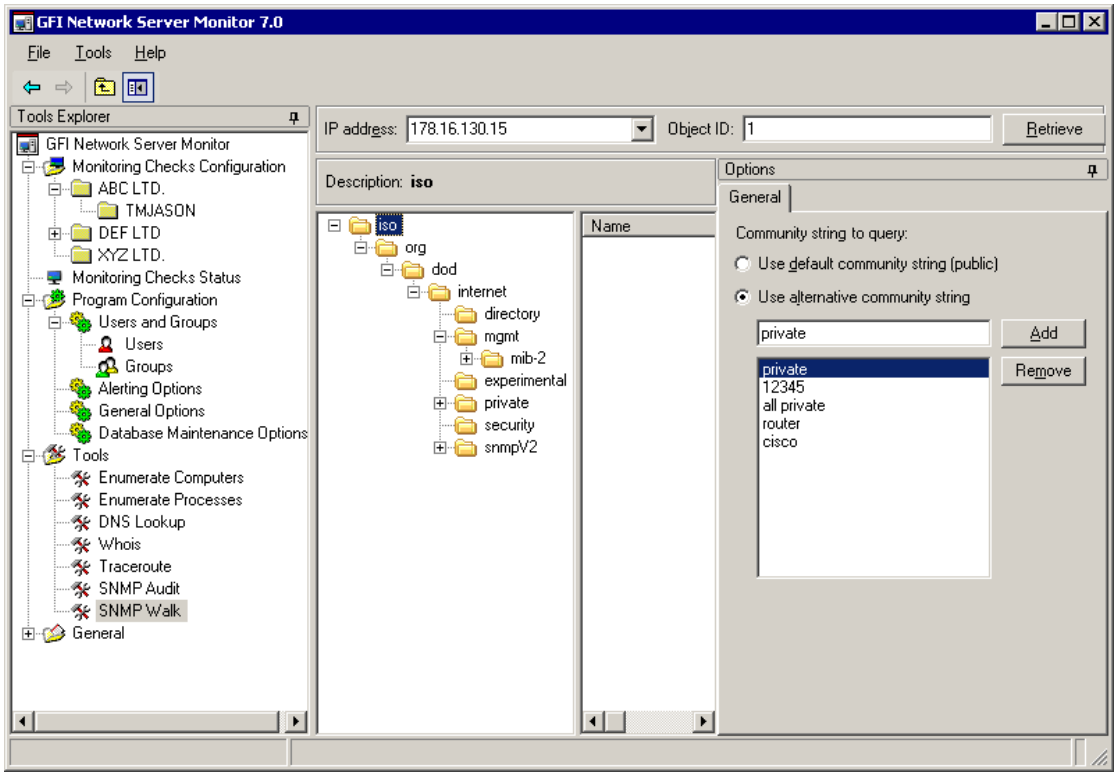
Screenshot 153 - The SNMP Audit tool

1. Specify the following parameters:
   - *IP* Address – The IP address of the computer running SNMP
   - String List –The list of strings/parameters to be checked (can be left as default). This property is by default set to the dictionary file included in GFI Network Server Monitor. This dictionary file called snmp-pass.txt contains the list of strings which forms the query data fields to be displayed in the result window, being the window on the right of the SNMP Audit setup window. Should more/less information be required, user can either edit the mentioned default file or create a new one using a text editor.
   - Resolve computer names – Enable this option to resolve IP addresses and display the computer name.
   - Scan Query Timeout – Timeout value in ms which defines the time that a query is allowed to run before being stopped
2. Click on 'Retrieve' to start SNMP audit.

12.7 SNMP walk

The SNMP walk allows you to gather SNMP information. The right pane contains a list of names symbolizing specific Object ID's on the device. To find out more about the information provided by the SNMP walk, you will have to check with the vendor. Some vendors provide great details on what each piece of information means, others, though their devices support SNMP, provide no documentation on it at all.

SNMP will help malicious users learn a lot about your system, making password guessing and similar attacks much easier. Unless this service is required it is highly recommended that SNMP is turned off.



Screenshot 154 - SNMP Walk Setup window

In most cases SNMP should be blocked at the router/firewall so that Internet users cannot SNMP scan your network.

It is possible to provide alternative community strings.

1. Specify the following parameters:
   - » IP address – Enter the IP address of a computer or device which you wish to scan/'walk'.
   - » Community String – (can be left as default) Define if the default Community string (public) or an alternative community string is to be used. Should it be required, key other alternative community strings.
2. Click on 'Retrieve' to start SNMP scan.

13 Other features

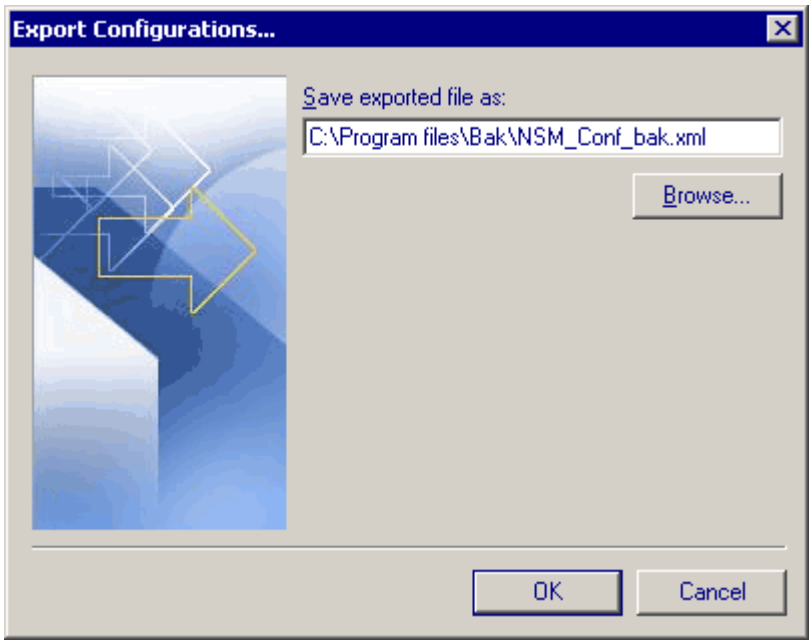
13.1 Export configurations

You can export a copy of your GFI Network Server Monitor configuration settings, including checks, folders alert settings, users/groups and general parameters to a specified XML file. This function can be used to backup your current configuration settings or to use the same configuration settings on another computer running GFI Network Server Monitor (e.g. to avoid reconfiguration when changing the computer on which GFI Network Server Monitor is running).

The Export Configuration function will export all configuration settings present in the GFI Network Server Monitor setup EXCEPT THE LICENSE KEY.

To export your configuration settings:

1. Go on File > Export Configurations.



Screenshot 155 - Export Configuration settings

2. Specify the location where the exported XML file will be placed (e.g. C:\Program Files\GFI\configBackup.xml) or click on 'Browse' to search for the location.

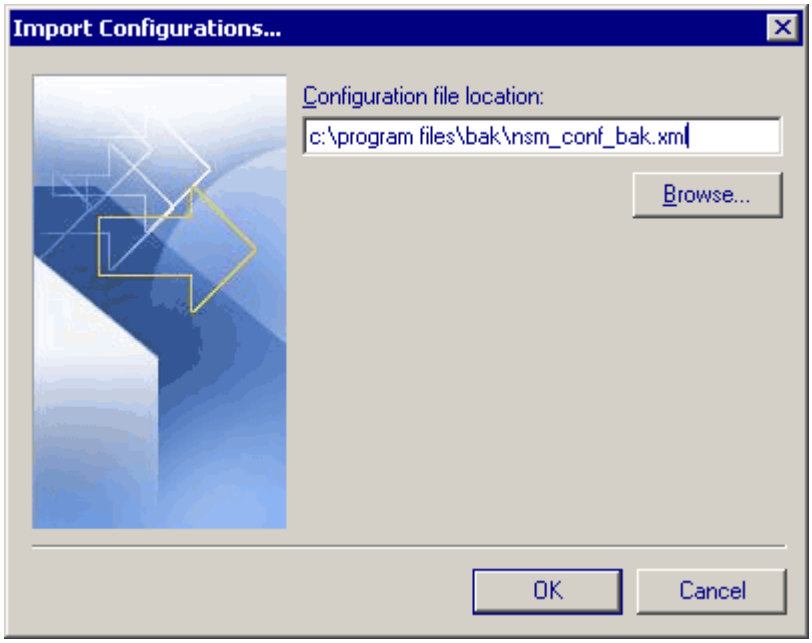
3. Click on 'OK' to save the file.

13.2 Import configurations

You can import all configuration settings (except for the license key) of another GFI Network Server Monitor setup (e.g., from another server) by using the Import configuration function. This function conveniently avoids having to re-configure the settings of GFI Network Server Monitor when you need to change the computer on which your current version of GFI Network Server Monitor is running.

Since importing a configuration will overwrite all your current configuration settings, we strongly recommend that you export a copy of your current configuration settings and keep it as a backup.

1. Go on File > Import Configurations.

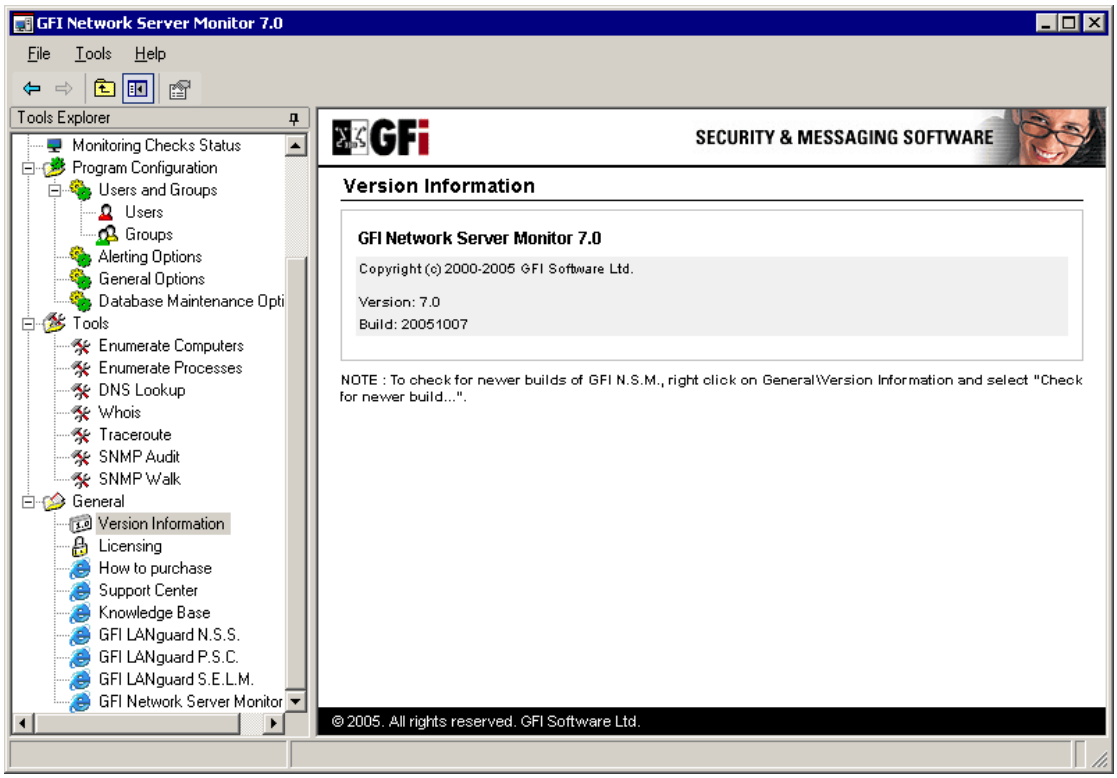


Screenshot 156 - Import configuration settings

2. Specify the complete path to the XML file containing the configuration settings (e.g. \\NSM_Server2\Program Files\GFI\config_Backup.xml) or click on 'Browse' to search for the file.

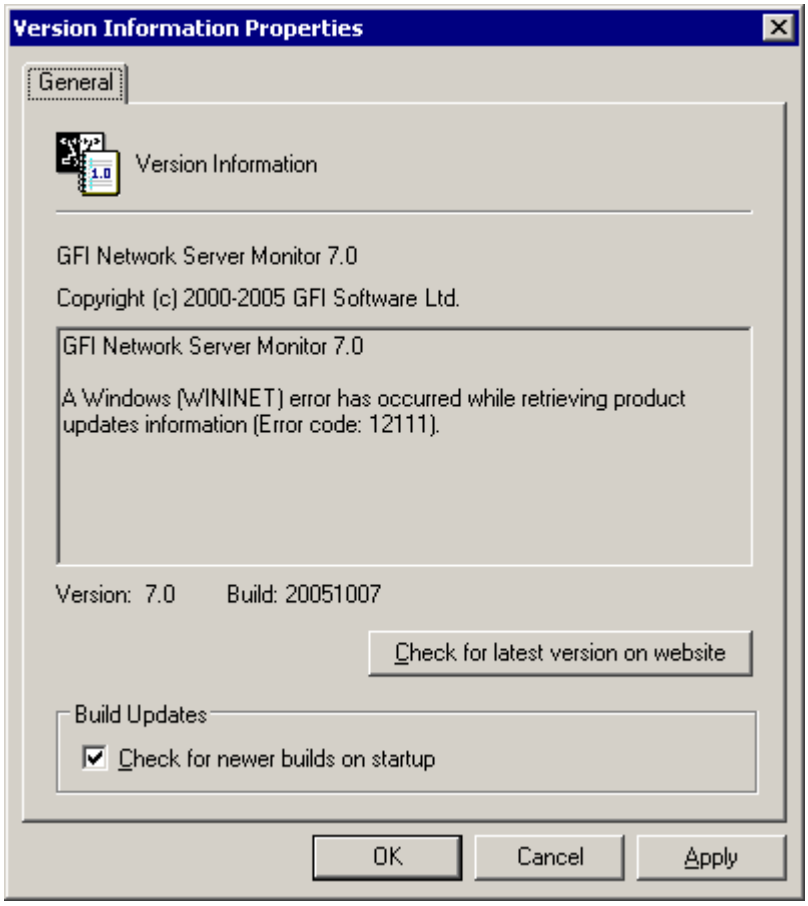
3. Click on 'OK' to import the specified configuration file.

13.3 Version information



Screenshot 157 - Version Information

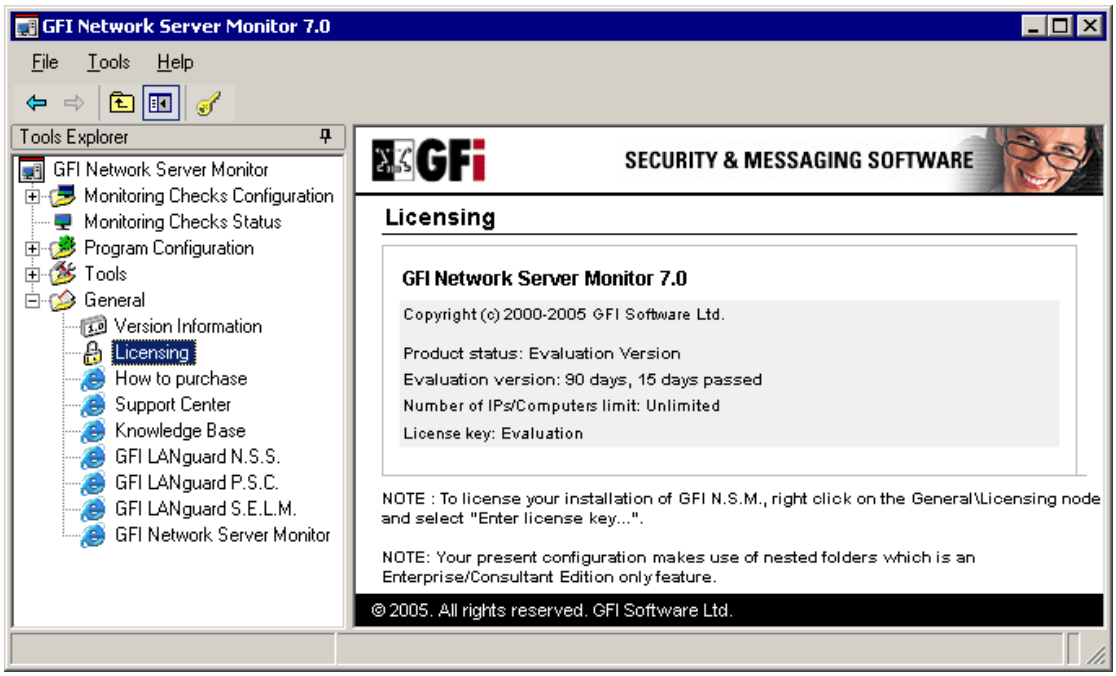
Check the version of GFI Network Server Monitor from 'General' node > 'Version Information'.



Screenshot 158 - Check for Newer Builds

To check for newer builds, right click on 'Version Information' in the 'General' Node and selecting 'Check for Newer Build…'

13.4 Licensing


GFI Network Server Monitor 7.0
File
Tools
Help
Tools Explorer
GFI Network Server Monitor
Monitoring Checks Configuration
Monitoring Checks Status
Program Configuration
Tools
General
Version Information
Licensing
How to purchase
Support Center
Knowledge Base
GFI LANguard N.S.S.
GFI LANguard P.S.C.
GFI LANguard S.E.L.M.
GFI Network Server Monitor
SECURITY & MESSAGING SOFTWARE
Licensing
GFI Network Server Monitor 7.0
Copyright (c) 2000-2005 GFI Software Ltd.
Product status: Evaluation Version
Evaluation version: 90 days, 15 days passed
Number of IPs/Computers limit: Unlimited
License key: Evaluation
NOTE : To license your installation of GFI N.S.M., right click on the General\Licensing node and select "Enter license key...".
NOTE: Your present configuration makes use of nested folders which is an Enterprise/Consultant Edition only feature.
© 2005. All rights reserved. GFI Software Ltd.

Screenshot 159 - Licensing details

To check your licensing details, click on 'Licensing' in the 'General' node.

14 Writing your own monitoring functions

14.1 Introduction

GFI Support cannot assist you in the writing and debugging of custom scripts. You must be familiar with VBscript to write your own functions and you must debug them yourself.

GFI Network Server Monitor is designed to let operators write their own monitor functions and use them in the product. GFI uses VBScript because it is the most popular scripting language in Windows environments.

GFI Network Server Monitor uses VBscript itself to perform a number of checks. In fact, during installation, five VBScript files are installed:

- ads.vbs – includes monitor functions based on ADSI (Active Directory Service Interfaces);
- exchange.vbs – includes monitor functions that can check Exchange 2000/2003 servers;
- hardware.vbs – includes hardware related monitor functions;
- os.vbs – includes Operating System related monitor functions;
- sample.vbs – includes some sample functions.

14.2 Writing a script/function

GFI Network Server Monitor functions should always return:

- -1 (True); Return -1 in case the Monitor Function is successful. For instance, if your function checks the existence of a certain directory, and it does exist, then return -1;
- 0 (False); Return 0 in case the Monitor Function is not successful. For instance, if your function checks the existence of a certain directory, and it does not exist, then return 0;
- 1 (Unknown); Return 1 in case the Monitor Function cannot determine True or False. For instance, if your function checks the existence of a certain directory on a server, but it cannot find the server at all (for instance because the computer is down), return 1;

It's very easy to write your own monitor functions in VBScript. Use the following guidelines when writing a new function:

- The routine must be a Function, not a Sub;
- The Function must return True (-1), False (0) or Unknown (1);
- Optionally, use the EXPLANATION system variable to add your own explanation to the result of the function; this EXPLANATION is shown in the client program each time the check is made;
- All variables must be 'dimmed', except EXPLANATION. EXPLANATION is a GFI Network Server Monitor system variable automatically dimmed by the GFI Network Server Monitor service.

The function must be written according to the following template:

```
Const retvalUnknown = 1
Function Function_i( var1, var2, ..., varn )
      If ( Not Pre-condition ) Then
            EXPLANATION = "Unable to determine..."
 Function_i = retvalUnknown
      Else
```

```
  If( condition ) Then
    EXPLANATION = "Yes it is true because ..."
    Function_i = True
  Else
            EXPLANATION = "No it's not true because ..."
    Function_i = False
  End If
      End If
End Function
```

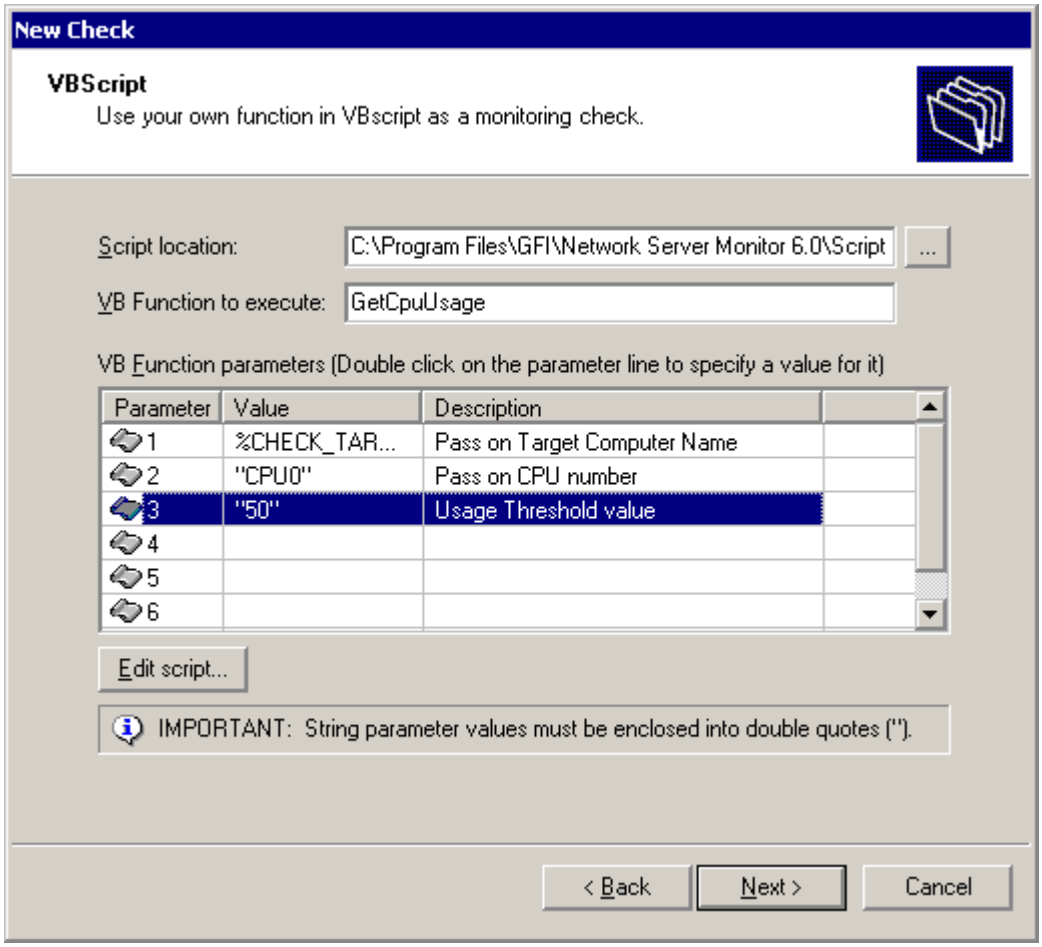
where Function_i is an arbitrary name for the function.

You can save this function in either one of the standard VBS files (i.e. ads.vbs, exchange.vbs, hardware.vbs, os.vbs or sample.vbs), or in a new VBScript file. In case of a new file ensure that your VBS file is accessible via the GFI Network Server Monitor Share.

14.3 Adding a monitor function written in VBscript

After you have written a monitor function in VBscript, you must add it in the Network Server Monitor Manager as a check. To do this:

1. Right Click on 'Monitoring Checks Configuration' and go on New > Monitoring Check.



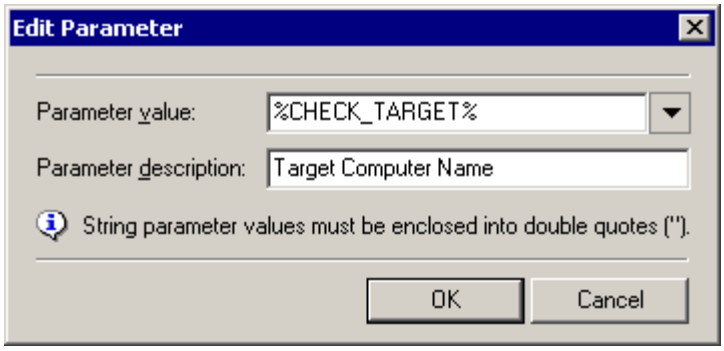
Screenshot 160 - VBscript check parameters dialog

2. Select 'Generic VB Script' and specify the following parameters:

- Script location – Specify the path to the VBScript file which will be used. The script should contain the function specified in the Function name field and should return True (-1) in case of success, or False (0) in case of an error;

- Function name – Specify the function that GFI Network Server Monitor service will be calling from the specified script file.
- VB Function Parameters – Double click on the line where the additional parameter values required by this function are to be specified.

Parameters will be passed to the function according to their position in the list, starting from 1.



Screenshot 161 - Add Parameters dialog

- Specify the parameter value and description. Parameter values can be extracted from system variables (e.g. %USERNAME%) upon execution of the function or directly specified as a string (e.g. “JasonM”)

Enclose string parameter values within quotes (e.g. “CPU0”).

You can make changes to the selected script by clicking on the ‘Edit script …’ button.

14.4 WMI (Windows Management Instrumentation)

If you plan to write monitor functions based on WMI (Windows Management Instrumentation), be sure you have WMI installed on the GFI Network Server Monitor server and on the target computer/server that you want to monitor.

WMI is by default included as part of the Windows 2000/2003 operating system only. For NT4 systems download the file (for free) from the Microsoft website;

GFI has collected more than a hundred WMI samples. You can use these samples as a base for new monitor functions that you write yourself. You can find them on the GFI website.

14.5 ADSI (Active Directory Service Interfaces)

GFI Network Server Monitor can check several Directory Services including Active Directory, and NTDS (NT4 SAM database) directory services.

You can program GFI Network Server Monitor to check user accounts (locked out, disabled, etc.), computer accounts, groups, group membership, organizational units, and so on.

If you plan to write monitor functions based on ADSI (Active Directory Service Interfaces), be sure you have ADSI installed on the GFI Network Server Monitor server and on the server that you want to monitor. ADSI allows you to access Windows 2000/2003 Active Directory, but also NT4 User information from the SAM database, and other User Databases. ADSI is part of the Windows

2000 operating system; and it's not part of NT4. For NT4, please download the file from the Microsoft website; ADSI is available for free.

GFI includes a sample script that uses ADSI, called ads.vbs. In addition, GFI provides some sample ADSI scripts on the website. You can use these samples as a base for new monitor functions that use ADSI.

15 Troubleshooting

15.1 Introduction

The troubleshooting chapter explains how you should go about resolving any software issues that you might encounter. The main sources of information available to users are:

- The manual – most issues can be solved by reading this manual.
- GFI Knowledge Base articles
- Web forum
- Contacting the GFI Technical Support

15.2 Knowledge Base

GFI maintains a Knowledge Base, which includes answers to the most common problems. If you have a problem, please consult the Knowledge Base first. The Knowledge Base always has the most up-to-date listing of technical support questions and patches. To access the Knowledge Base, visit **http://kbase.gfi.com/**.

15.3 Web Forum

User to user technical support is available via the web forum. The forum can be found at: **http://forums.gfi.com/**.

15.4 Request technical support

If you have referred to this manual and our Knowledge Base articles, and you still cannot solve issues with the software, contact the GFI Technical Support team by filling in an online support request form or by phone.

- Online: Fill out the support request form on: http://support.gfi.com/supportrequestform.asp. Follow the instructions on this page closely to submit your support request.
- Phone: To obtain the correct technical support phone number for your region please visit: **http://www.gfi.com/company/contact.htm**.

Before you contact our Technical Support team, please have your Customer ID available. Your Customer ID is the online account number that is assigned to you when you first register your license keys in our Customer Area at: **http://customers.gfi.com**.

We will answer your query within 24 hours or less, depending on your time zone.

15.5 Build notifications

We strongly suggest that you subscribe to our build notifications list. This way, you will be immediately notified about new product builds. To subscribe to our build notifications, visit: **http://www.gfi.com/pages/productmailing.htm**.

Index

A

ADSI, 4, 165, 167, 168

Alerting Options, 104, 105, 106, 107, 108, 111, 113, 114, 117, 119, 121, 123, 124

alerts, 1, 5, 12, 32, 35

Alerts, 25, 26

C

Check folders, 35, 93

checks status, 97

configuration, 13, 23, 24, 29, 30, 31, 33, 34

CPU usage, 2, 4

D

database backend, 2, 12, 137, 138, 139, 147

Dependencies, 31, 32

Directory size, 3, 4

Disk drive, 3

Disk space, 2, 4

DNS server, 3, 47

E

email, 1, 35, 104, 106

EMAIL, 141

e-mail alerts, 25, 26

Event ID, 2, 61, 62

Event Log, 62

Event Log function, 2

Exchange, 2

F

File existence, 2, 4, 63

File size function, 3, 4

FTP, 3, 40, 41

functional parameters, 23

G

general parameters, 22, 142, 161

GSM, 110, 125

H

HTTP function, 3

I

ICMP ping, 3

inheritance, 1

installation, 7, 10, 13, 130, 133, 165

L

License, 6

Linux / Unix OS generic checks, 80

Linux/Unix Operating System Checks, 82

logon credentials, 12, 20, 23, 40, 106, 155

Logon Credentials, 13, 23, 39, 40, 41, 155

M

Maintenance, 33, 34

maintenance periods, 5, 34

maintenance schedule, 34

Message Templates, 124, 125

Monitoring Check Wizard, 17

N

nested folders, 1, 2

Nested folders, 2, 93

network alerts, 25

Network Alerts, 26

network message., 1

Network Monitor Engine, 1, 5, 56, 118

Network Monitor Manager, 6

Network Support Tools, 4

Network tools, 153

Network/Internet monitor functions, 39

NNTP, 3, 42, 43

NTP, 3, 45, 46

P

pager, 1

Pager, 25, 125

Physical Disk Condition function, 3

POP3, 3, 43

Printer availability function, 3, 4

Process Running function, 3, 4

Properties, 60, 61, 65, 94, 95, 105, 106, 107, 108, 111, 113, 114, 117, 119, 121, 123, 124, 128, 129, 134, 135, 137

property inheritance, 1, 34

Q

Quick Start Wizard, 1, 14

R

Reporting, 5

reporting tool, 147

reports, 5, 147

S

Services function, 2

SMS, 1, 25, 26, 109, 118, 119, 121, 122, 123, 124, 125

SMSC, 1, 118, 120, 121, 122, 123

SMTP server, 3, 26, 45

SNMP, 3, 55, 56, 103

SNMP monitoring checks, 55

SQL, 2

state indicators, 103

System requirements, 7

T

TCP, 3, 41, 42, 43, 44, 45, 48, 49

Terminal Services checks, 78, 79, 80

U

uncertain result, 103, 127

UNIX, 1

Users and Groups, 3, 4, 28, 73, 88, 108, 141, 145, 146

Users and Groups Membership function, 3, 4

V

VBScript, 4, 57, 165, 166

W

Windows applications checks, 73

Windows operating system checks, 61

Windows OS databases checks, 76

Windows OS generic checks, 56

WMI, 4, 61, 167

working hours, 1, 2, 141, 142, 143, 144

X

XML, 5, 147

USA, CANADA, CENTRAL AND SOUTH AMERICA

15300 Weston Parkway, Suite 104, Cary, NC 27513, USA

Telephone: +1 (888) 243-4329

Fax: +1 (919) 379-3402

Email: ussales@gfi.com

UK AND REPUBLIC OF IRELAND

Magna House, 18-32 London Road, Staines, Middlesex, TW18 4BP, UK

Telephone: +44 (0) 870 770 5370

Fax: +44 (0) 870 770 5377

Email: sales@gfi.co.uk

EUROPE, MIDDLE EAST AND AFRICA

GFI House, San Andrea Street, San Gwann, SGN 1612, Malta

Telephone: +356 2205 2000

Fax: +356 2138 2419

Email: sales@gfi.com

AUSTRALIA AND NEW ZEALAND

83 King William Road, Unley 5061, South Australia

Telephone: +61 8 8273 3000

Fax: +61 8 8273 3099

Email: sales@gfiap.com